Ilari Käyhkö

LOHKOKETJUTEKNOLOGIA RAHOITUSPALVELUISSA

Kandidaatintutkielma

Kauppatieteet

Toukokuu 2021

SISÄLLYS

KUVIOT

1 JOHDANTO

Teollinen vallankumous alkoi 1700- ja 1800-lukujen vaihteessa Britanniassa ja käynnisti höyrykoneen avulla laajan yhteiskunnallisen, taloudellisen ja teknologisen murroksen lähes koko maailmassa. Tämän jälkeen koettiin toinen teollinen vallankumous sähkön, maakaasun ja öljyn energianlähteeksi valjastamisen myötä 1870-luvulla. Kolmas teollinen vallankumous alkoi mikropiirin keksimisestä 1900-luvun lopulla, minkä avulla kehittyivät muun muassa elektroniikka, tietoliikenne ja tietokone. Tällä hetkellä eletään neljännen teollisen vallankumouksen aikaa, jonka keskeisin muutosvoima on internet. Muita keskeisiä neljänteen teolliseen vallankumoukseen liittyviä innovaatiota ovat muun muassa esineiden internet eli IoT (internet of things), pilvipalvelut ja koneoppiminen. (Jensen, 1993; Schwab, 2017, s. 6–7.)

Kaikelle teknologiselle kehitykselle on ominaista se, että uudet teknologiat perustuvat aina osittain aikaisempiin teknologioihin ja innovaatioihin. Tilikirjoja ja julkisia rekistereitä on todistettavasti käytetty jo yli 5000 vuotta sitten muinaisessa Mesopotamiassa, ja esimerkiksi kirjanpito itsessään on kymmeniä tuhansia vuosia vanha ala (Benzel, Graff, Rakic & Watts, 2010, s. 58–59). Noista ajoista tultiin sulkakynällä pergamentille kirjoitettuihin julkisiin rekistereihin ja kahdenkertaiseen kirjanpitoon, joita käytettiin kylissä ja kaupungeissa muun muassa ostojen, myyntien, syntymien, kuolemien, lainojen, avioliittojen sekä kaiken muun tärkeän kirjaamiseen. Lohkoketju (blockchain) on kehittynyt digitaalinen versio tällaisesta julkisesta rekisteristä tai tilikirjasta, aivan kuten tietokonekin on käytännössä vain kehittyneempi versio Antikytheran koneesta[1]. Lohkoketjun toiminnan keskeisimmät osat ja teknologiat eivät välttämättä ole uusia, mutta lohkoketju itsessään on uusi teknologia. Se tulee olemaan osa nykyistä neljättä teollista vallankumousta internetin, IoT:n ja sosiaalisen median ohella, vaikka sen asema ei vielä ole vakiintunut.

[1] Antikytheran kone on antiikin Kreikan ajoilta peräisin oleva maailman vanhin esimerkki analogiatietokoneesta.

Lohkoketju on tänä päivänä hyvin trendikäs sana, joka yhdistyy ihmisten mielissä suoraan tunnettuun virtuaalivaluuttaan bitcoiniin. Vaikka lohkoketjuteknologia suunniteltiin alun perin toiminta-alustaksi bitcoinille, lohkoketju ja bitcoin eivät ole toistensa synonyymeja. Yksi tämän kandidaatintutkielman tavoite onkin tuoda esille, että lohkoketjuteknologiaa voidaan hyödyntää paljon laajemmassa kontekstissa kuin vain virtuaalivaluutoissa. Käyttökohteiden aihepiiri rajataan rahoituspalveluihin, sillä varsinkin vuoden 2008 finanssikriisin jälkeen on huomattu, että vaihtoehtoisten ratkaisujen löytäminen rahoitusalalla on enemmän kuin tarpeen. Lisäksi käydään tarkemmin läpi, mitä vahvuuksia ja haasteita lohkoketjuteknologia kohtaa ominaisuuksiensa puolesta nyt ja tulevaisuudessa. Toinen tutkielman tavoite on selvittää, miten näiden ominaisuuksien kautta voidaan parantaa rahoituspalveluiden toteuttamista. Tavoitetta lähestytään esittelemällä erilaisia käyttökohteita, ja miten kohteita voidaan laajentaa jatkossa.

Lohkoketjuteknologiaa on tutkittu selvästi vähemmän kuin perinteisempiä teknologioita. Lohkoketjuun liittyvää kirjallisuutta ja opinnäytetöitä on saatavilla varsin vähän. Tämän vuoksi tutkimusaihe on houkutteleva, sillä sen avulla päästään tuottamaan mahdollisesti lisäarvoa yliopistoissa suomeksi kirjoitettuun tutkimukseen. Tämän tutkielman päämäärä on esitellä lukijalle, mitä lohkoketjuteknologia tarkoittaa, ja miten sitä voidaan soveltaa rahoituspalveluissa. Tutkielmassa korostetaan erityisesti lohkoketjuteknologian rakennetta ja ominaisuuksia, jotta sen käyttökohteet voidaan paremmin hahmottaa.

Tärkeimpiä tutkimuskysymyksiä ovat:

1) Mitä lohkoketjuteknologia on?
2) Mitä eri ominaisuuksia lohkoketjuteknologialla on, eli mitä vahvuuksia ja haasteita lohkoketjuteknologia kohtaa?
3) Miten lohkoketjuteknologiaa on jo hyödynnetty rahoituspalveluissa, ja miten sitä voidaan tulevaisuudessa hyödyntää?

Tärkeimmät käytettävät tutkimusmenetelmät ovat aiheeseen liittyvän olemassa olevan kirjallisuuden tutkimus sekä sen soveltaminen eri asiayhteyksissä. Kirjallisena

aineistona käytetään aiheeseen liittyviä kirjoja, vertaisarvioituja tieteellisiä artikkeleita, tilastoja, raportteja sekä asiantuntijoiden omia lausuntoja.

Tutkielmassa tarkastellaan lohkoketjun rakennetta hajautettuna tilikirjana, jonka kryptografiset[2] periaatteet ja hajautettu tietoverkkorakenne mahdollistavat sen luotettavuuden, avoimuuden, tiedon eheyden sekä turvallisuuden. Vaikka lohkoketju toimii ilman keskitettyä tietoverkkoarkkitehtuuria tai keskusviranomaista, vallitsee sen sisällä silti yhteisymmärrys tiedon oikeellisuudesta ja varmennuksesta. Lohkoketjun monipuolisiin ja tietyllä tapaa mullistaviin ominaisuuksiin liittyvät hyödyt ovat tehneet siitä houkuttelevan vaihtoehdon tyypillisten rahoituspalveluiden toteuttamiseen. Hajautettu tietoverkko sekä älykkäät sopimukset voivat mullistaa esimerkiksi maksujärjestelmät, osakekaupan tehokkuuden ja sisäiset hallintojärjestelmät. Lohkoketjuteknologia on kuitenkin uusi teknologia, joten se kohtaa myös epävarmuutta teknisistä ongelmista, mahdollisesta sääntelystä sekä hitaasta omaksumisesta johtuen. Nämä kaikki ovat asioita, jotka tulee ottaa huomioon rahoituspalveluita suunniteltaessa.

Toisessa pääluvussa esitellään lohkoketjuteknologiaa käsitteenä yleisellä tasolla ja tarkastellaan sitä suhteessa teknologisen kehityksen ja sen omaan historiaan. Kolmannessa pääluvussa tarkastellaan lohkoketjun rakennetta sen pienimmistä osista alkaen siinä hyödynnettyihin toimintaperiaatteisiin asti. Neljännessä pääluvussa tarkastellaan eri lohkoketjuteknologiaan liittyviä ominaisuuksia, kuten vahvuuksia ja haasteita. Viidennessä pääluvussa esitellään lohkoketjuteknologian nykyisiä ja tulevia käyttökohteita rahoituspalveluissa. Viimeinen eli kuudes pääluku on yhteenveto tutkielman aikana esiintyneistä tärkeimmistä huomioista koskien lohkoketjuteknologian hyödyntämistä rahoituspalveluissa.

[2] Kryptografia tai kryptologia[2], eli salakirjoitustekniikka, tarkoittaa turvallisen viestinnän menetelmien tutkimista ja harjoittamista kolmansien osapuolien eli vastustajien läsnä ollessa.

2 YLEISTÄ LOHKOKETJUTEKNOLOGIASTA

2.1 Lohkoketjun lyhyt historia

Lohkoketju kehiteltiin vuonna 2008, kun Satoshi Nakamoto -nimimerkillä toiminut taho julkaisi internetissä niin kutsutun white paperin[3] nimeltään *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008). Kukaan ei toistaiseksi tiedä, kuka Nakamoto on tai oli, vaikka asiaa on tutkittu jo usean vuoden ajan. Suosituimman teorian mukaan Nakamoto on useamman eri toimijan käyttämä yhteinen salanimi, jonka avulla toimijoiden tai toimijan anonymiteetti säilytetään. Julkaisu oli ajallisesti hyvin merkittävä, sillä se ilmestyi juuri vuosien 2007–2008 finanssikriisin loppuvaiheessa. Globaali talouskriisi oli merkittävästi horjuttanut ihmisten luottamusta nykyistä talousjärjestelmäämme kohtaan, ja se lähti liikkeelle Yhdysvalloista luottokuplan puhjettua. Tähän mennessä suurten pankkien tilikirjat olivat muuttuneet niin vaikeasti hallittaviksi, että pankeilla ei ollut täyttä varmuutta edes niiden varallisuuden todellisesta arvosta markkinoilla. Uskotaan, että tätä selitti etenkin pankkien käyttämien omien kirjanpitojärjestelmien ja teknologioiden skaalautuvuuden puute. Nakamoto uskoo, että bitcoin ja lohkoketju ratkaisisivat edellä mainitut ongelmat ja estäisivät seuraavan tulevan talousromahduksen tai laman.

Sähköinen rahajärjestelmä bitcoin on historian ensimmäinen lohkoketju, joka perustuu Nakamoton (2008) esittämään ajatukseen järjestelmästä, joka mahdollistaa sähköiset transaktiot suoraan vertaiselta vertaiselle ilman keskitettyä ja luotettua kolmatta osapuolta[4]. White paperin keskeisenä pääajatuksena oli nykyiseen rahajärjestelmään liittyvät luottamusongelmat, sillä suurin osa sähköisistä transaktioista nojasi pitkälti taloudellisiin instituutioihin, jotka toimivat luotettuina kolmansina osapuolina maksujen prosessoinnissa. Seuraava lainaus on vapaa suomennos white paperin johdanto-osasta: Täysin peruuttamattomat transaktiot eivät ole (nykyisessä rahajärjestelmässä) juuri mahdollisia, sillä taloudelliset instituutiot eivät voi välttyä

[3] White paper on julkaisu, jonka avulla voidaan esittää lukijalle helposti omaksuttavassa muodossa jokin kanta tai ratkaisu johonkin tiettyyn ongelmaan.
[4] Luotettu kolmas osapuoli eli TTP (Trusted Third Party) tarkoittaa turvallisuusviranomaista tai tämän valtuuttamaa tahoa, johon käyttäjät luottavat ja joka tarjoaa tietoturvallisuuteen liittyviä palveluja.

riitatilanteiden sovittelulta. Näiden riitatilanteiden sovittelu lisää transaktiokustannuksia, mikä puolestaan vähentää pienimmän mahdollisen transaktion kokoa ja estää näin pienet satunnaiset transaktiot. Tästä aiheutuu vielä suurempi kustannus, kun menetetään kyky tehdä peruuttamattomia maksuja peruuttamattomista palveluista. Täten mahdollinen maksun peruuttaminen aiheuttaa suuremman tarpeen luottamukselle. Tietty prosenttimäärä petoksista hyväksytään välttämättöminä, ja lisäksi kauppiaiden tulee olla varuillaan, etteivät pyydä asiakkaistaan enemmän tietoa kuin muuten tarvittaisiin. (Nakamoto, 2008)

Nakamoton (2008) esittämille ongelmille löytyisi ratkaisu fyysisen valuutan käyttämisestä, mutta sen sijaan sähköiset transaktiot eivät ole onnistuneet ilman luotettua kolmatta osapuolta. Tähän Nakamoto esittää vastaukseksi elektronista maksujärjestelmää, joka perustuu kryptografiselle todisteelle luottamuksen sijasta, mahdollistaen transaktioiden suorittamisen minkä tahansa kahden osapuolen välillä ilman luotettua kolmatta osapuolta. Tämä maksujärjestelmä loi pohjan lohkoketjuteknologialle sellaisena kuin se nykyään tunnetaan.

2.2 Makrotason määritelmät

Rahoituksen ala on ollut jo pitkään teknologisessa murroksessa, joten on luontevaa tarkastella siihen liittyviä palveluita myös uuden teknologian näkökulmasta. Lohkoketju on suhteellisen tuore keksintö, mutta se saattaa tarjota pysyviä ratkaisuja haasteisiin, jotka ovat olleet jo pitkään yleisiä eri palveluiden toteutuksessa. Sitä voitaisiin kutsua vakiintuneita toimintamalleja murtavaksi teknologiaksi eli *disruptiiviseksi teknologiaksi* (disruptive technology) määritelmän klassisen tulkinnan mukaan (Bower & Christensen, 1995). Tällainen disruptiivinen teknologia kasvattaa tuottavuutta markkinoilla, mutta aluksi sen tulevaisuuden näkymiä kyseenalaistetaan. Ajan myötä se kuitenkin vakiintuu markkinoille syrjäyttäen kalliimmat ja hitaammat rakenteet sekä toimintamallit tehokkaan kustannusrakenteensa ansiosta. Monet asiantuntijat uskovat lohkoketjun mullistavan rahoitus- sekä pankkialan aivan kuten internet ja sosiaalinen media ovat mullistaneet tietoliikenteen ja viestinnän viimeisen kahden vuosikymmenen aikana (Swan, 2015, s. ix). Tässä tapauksessa ei ole kyse enää disruptiivisesta teknologiasta vaan *perustavanlaatuisesta teknologiasta* (foundational technology). Perustavanlaatuinen teknologia ei pelkästään tarjoa uutta

kustannustehokasta ratkaisua ja liiketoimintamallia, vaan se luo kokonaan uuden pohjan taloudellisille ja poliittisille järjestelmille (Iansiti & Lakhani, 2017).

Jotkut asiantuntijat, kuten tunnettu taloustieteilijä Nouriel Roubini (2018), taas pitävät lohkoketjuteknologiaa yhtenä yliarvostetuimmista teknologioista koskaan. Myös Deloitten (2020) laatimassa tuoreessa kyselyssä lähes 51 prosenttia yli tuhannesta vastanneesta kansainvälisestä johtohenkilöstä piti lohkoketjuteknologiaa yliarvostettuna, vaikka 88 prosenttia uskoikin sen laajempaan omaksumiseen tulevaisuudessa. Lohkoketjun käyttöönotto ei kuitenkaan tule tapahtumaan yhtä nopeasti ja yhtäkkisesti kuin esimerkiksi sosiaalisen median, vaan enemmänkin vaiheittain ja hitaasti. Voi olla, että lohkoketju ei koskaan saavuta kohtaamiaan odotuksia. Toisaalta on myös muistettava, että internet kehitettiin 1960-luvulla, mutta se popularisoitui vasta 1990-luvun puolivälissä eli tämän innovaation kypsymiseen meni yli kolme vuosikymmentä. Vain aika näyttää, onko lohkoketju perustavanlaatuinen teknologia, sillä suuret muutokset eivät yleensä tapahdu yhdessä yössä.

Sana *lohkoketju* tulee Nakamoton (2008) white paper -julkaisusta, jossa kirjoittaja käytti termiä *chain of blocks*. Sana *lohko* viittaa transaktioiden liittämiseen kryptografisesti yhteen omaksi yksikökseen eli lohkoksi, ja sana *ketju* taas näiden lohkojen ketjuttamiseen toisiinsa. On kuitenkin olemassa lohkoketjuja, joissa ei synny ollenkaan lohkoja, joten tässä mielessä termi voi olla hieman harhaanjohtava (Johansson, Eerola, Innanen & Viitala, 2019, s. 27). Lisäksi joissain asiayhteyksissä lohkoketjuteknologiasta käytetään myös nimitystä *hajautetun tilikirjan teknologia* (distributed ledger technology eli DLT), mutta lohkoketju on pikemminkin vain yksi hajautetun tilikirjan ilmentymismuoto. Hajautetussa tilikirjassa ei välttämättä ole ollenkaan lohkoketjulle tyypillisiä dataa sisältäviä lohkoja tai edes ketjua lohkojen välillä. Käytännössä siis kaikki lohkoketjut ovat hajautettuja tilikirjoja, mutta kaikki hajautetut tilikirjat eivät ole lohkoketjuja. Hajautetun tilikirjan merkittävin ominaisuus ja piirre on sen hajautetun tietoverkon ja tietokannan rakenne.

Lohkoketju muodostuu esimerkiksi sen käyttäjien välisistä transaktioista siten, että järjestelmä kasaa yhteen useita eri käyttäjien välisiä transaktioita tai dataa yhtä aikaa

ja muodostaa niistä lohkoja. Lohkoon mahtuu tietyn verran dataa[5], ja kun se täyttyy, sen sisältö varmennetaan ja se linkitetään tiivistefunktion (hash function) avulla sitä edeltäneeseen lohkoon. Tästä syntyy ketju linkitettyjä lohkoja eli lohkoketju. Lohkoketju voidaan myös määritellä julkisena tapahtumarekisterinä, jonka luotettavuus perustuu kryptografiselle todisteelle eikä kolmannen osapuolen, kuten ihmisen ylläpitämän keskusviranomaisen tekemälle lupaukselle (Nakamoto, 2008). Se, että lohkoketjua ei hallinnoi jokin tietty keskitetty instituutio, kuten pankki tai valtion organisaatio, on lohkoketjun tunnunsomaisin piirre. Lohkoketju tallennetaan yhtä aikaa eri kopioina usealle erilliselle itsenäiselle laitteelle, jotka yhdessä ylläpitävät tietoja samassa verkossa. Jokainen verkossa lohkoketjua ylläpitävä laite voi muokata sitä niin kutsutun konsensusprotokollan[6] puitteissa. Konsensusprotokolla vaatii kaikkien verkon toimijoiden yhteisymmärryksen eli konsensuksen. Ilman konsensusta yksittäisen toimijan muokkaus hylätään, mutta hyväksyttäessä muokkaus päivitetään yhtä aikaa kaikkien toimijoiden omiin kopioihin tilikirjasta.

Lohkoketjulle ei ole yhtä tarkkaa määritelmää, vaan määritelmä riippuu täysin tilanteesta ja käyttökontekstista. Selkein lyhyt kuvaus lohkoketjusta on luotettava julkinen digitaalinen tilikirja, johon merkitään erilaisia tapahtumia aikajärjestyksessä. Tämä tilikirja hyödyntää toimintansa pohjana kehittynyttä kryptografiaa ja hajautettua järjestelmäarkkitehtuuria.

[5] Esimerkiksi bitcoinin lohkoketjussa yhteen lohkoon mahtuu keskimäärin 1000–3000 transaktiota (Blockchain.com, 2021).

[6] Konsensusprotokolla tarkoittaa yhteiskäytäntöä eli yhteisymmärryksen takaavaa käytäntöä tai standardia. Tämän tueksi on olemassa eri konsensusalgoritmeja eli matemaattisia mekanismeja, joilla konsensus saavutetaan.

3 LOHKOKETJUN RAKENNE

3.1 Hajautettu toimintaympäristö

Suurin osa tunnetuista tietoverkoista pohjautuu niin kutsuttuun keskitettyyn tietoverkkoarkkitehtuuriin. Tämä tarkoittaa sitä, että esimerkiksi verkko käyttää fyysistä keskuspalvelinta, johon kaikki verkossa olevat laitteet ovat yhteydessä ja johon kaikki sisäverkon tiedot ovat tallennettuina. Keskitetyn järjestelmän eräitä hyviä puolia ovat sen hyvä suorituskyky ja helppo ongelmanratkonta sekä rakennettavuus. Lisäksi siihen pääsee usein helposti käsiksi fyysisen sijaintinsa puolesta. Vastaavasti järjestelmän heikkous on se, että kaikki data on samassa paikassa, jolloin riski tietojen odottamattomalle menetykselle on huomattava. Lisäksi yksittäiset hyökkäykset keskuspalvelinta vastaan voivat kaataa koko verkon toiminnan.

Lohkoketju toimii hajautetun tietoverkon periaatteella. Hajautetun tietoverkon toinen nimi on P2P-verkko (peer-to-peer network) eli vertaisverkko. Kaikki vertaisverkkoon liittyneet solmut eli noodit[7] jakavat tietoa keskenään ja voivat myös kommunikoida muiden solmujen kanssa. Tässä tapauksessa tieto ei siis kulje yhden keskuspalvelimen kautta eikä verkko näin ollen ole riippuvainen yhdestä palvelimesta, joka voisi kaatua esimerkiksi hyökkäyksen tai luonnonvoimien takia. Yksi lohkoketjun perusajatuksista on, että jokaisella verkon solmulla on samat tiedot lohkoketjun sisältämästä datasta kuin kaikilla muillakin solmuilla, eli jokaisella verkon toimijalla on identtiset kopiot lohkoketjun tiedoista. Mikäli lohkoketjun tietoja päivitetään tai muokataan, tämä muutos tapahtuu myös jokaisen verkossa toimijan omassa kopiossa, ja näin ollen verkon yhteisymmärrys eli konsensus säilyy. Lohkoketjua voikin tässä tapauksessa kutsua kaikille verkon toimijoille tallennetuksi hajautetuksi tietokannaksi.

Tietokanta on dataa varastoiva kokonaisuus, jota useat toimijat voivat käyttää ja jota käsitellään yhteisenä joukkona keskitetysti, eli tietokanta sijaitsee yhdessä paikassa.

[7] Solmu eli noodi on tietoverkon yhteyspiste, joka sisältää dataa ja on yhteydessä muihin solmuihin. Internetissä mikä tahansa siihen yhdistynyt IP-osoitteellinen on solmu, kuten esimerkiksi tietokone tai älypuhelin. Täysi solmu (full node) sisältää täydellisen kopion kaikesta datasta lohkoketjussa, osittainen solmu (partial node) sen sijaan vain osittaisen kopion lohkoketjusta.

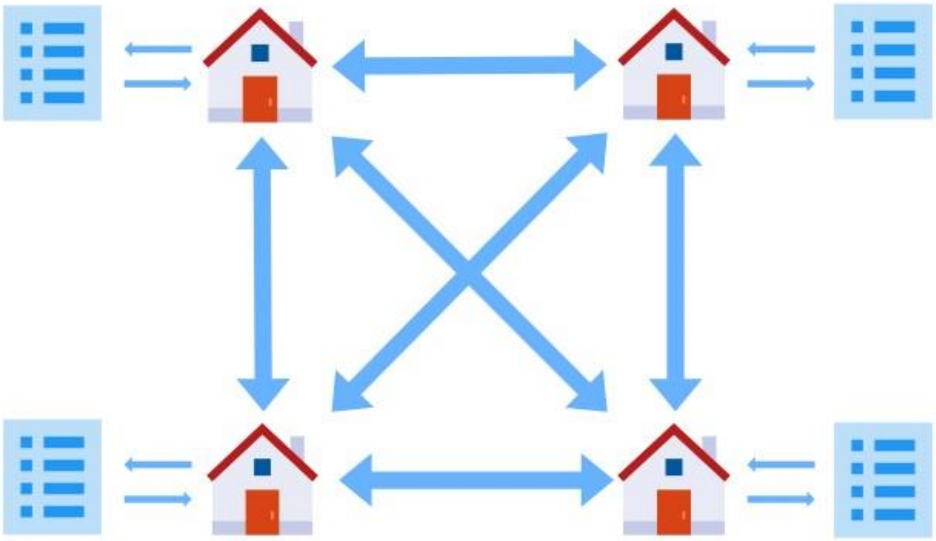
IBM loi ensimmäiset digitaaliset tietokannat 1970-luvulla, ja niiden merkitys on suuri vielä tänäkin päivänä. Tietokantoja tarvitaan lähes jokaisella yhteiskunnan osa-alueella tiedon varastoimiseen sekä hakemiseen, ja alun perin IBM:n laatima tietokantamalli onkin pysynyt lähes muuttumattomana kymmeniä vuosia. (Johansson, Eerola, Innanen & Viitala, 2019, s. 243.) Lohkoketju on kuitenkin muokannut perinteistä käsitystä tietokannoista. Lohkoketju on tietokanta, joka toimii hajautetussa verkossa, johon periaatteessa kuka tahansa voi liittyä. Tällä tavoin eri osapuolet voivat toimia keskenään ilman välikäsiä ja keskitettyä kolmatta osapuolta. Hajautettu tietoverkko tai hajautettu tietokanta ei varsinaisesti ole uusi keksintö[8], mutta lohkoketjussa nämä kaksi asiaa yhdistyvät uudella tavalla.

Lohkoketjun varsinainen perusyksikkö on hajautettu tilikirja (distributed ledger), joka on julkinen tapahtumarekisteri, johon kaikki lohkoketjun data tai suoritetut transaktiot ovat tallennettu. Hajautettu tilikirja on siis jaettu tietokanta, jonka henkilökohtaista kopiota verkon toimija voi hallita erillään muista. Kaikille verkon toimijoille jaettava kopio on identtinen, mutta jokaisen tulee päivittää se itsenäisesti. Jotta verkkoon osallistuneiden kesken jaetuista tiedoista päästäisiin yhteisymmärrykseen eli konsensukseen, tarvitaan niin kutsuttuja konsensusalgoritmeja. Kun konsensus on saavutettu, verkon toimijat päivittävät uuden datan hajautettuun tilikirjaan ja ne tallennetaan kryptografisesti varmennettuun ketjuun, jota ei voi enää sen jälkeen muuttaa tahallaan tai vahingossa. Jotta lohkoketjun tiedot voidaan päivittää, on verkon toimijoiden saavutettava ensin uusi konsensus, mikä takaa tiedon paremman eheyden hajautetussa järjestelmässä.

Kuvio 1 esittää hajautetun tilikirjan rakenteen, jossa eri toimijat ovat toisiinsa yhteydessä vertaisverkossa sen sijaan, että tieto siirtyisi yhteen suuntaan esimerkiksi yhdelle keskuspalvelimelle. Tässä tapauksessa tiedonsiirtoa kuvaavat nuolet, joista huomataan, että tieto liikkuu eri toimijoiden välillä joka suuntaan. Lisäksi jokaisella vertaisverkon toimijalla on oma kopionsa tilikirjasta, jota jokainen toimija voi hallita

[8] Hajautettu tietokanta on klassiselta määritelmältään maantieteellisesti hajautettu, eli se näyttäytyy käyttäjälleen yhtenä tietokantana mutta koostuu erillisistä tietokannoista eri laitteilla.

erillään muista. Keskitetyn tilikirjan tapauksessa rekisteristä olisi vain yksi kopio, jota ainoastaan keskuspalvelin voi hallita.



Kuvio 1: Hajautettu tilikirja.

3.2 Lohkoketjun kryptografia ja salaus

3.2.1 Kryptografia

Kryptografia tai kryptologia[9], eli salakirjoitustekniikka, tarkoittaa turvallisen viestinnän menetelmien tutkimista ja harjoittamista kolmansien osapuolien eli vastustajien läsnä ollessa (Rivest, 1990). Kryptografia miellettiin ennen modernin kryptografian aikaa synonyymina salaukselle. Salaus on tapa muuttaa viesti lukukelvottomaksi, jolloin vain viestin toivottu vastaanottaja pystyy kääntämään sen takaisin lukukelpoiseksi. Tieto siitä, miten viesti tulisi lukea toimii avaimena, jonka avulla viesti voidaan joko salata tai avata. Muun muassa antiikin Roomassa Julius Caesar käytti sotasalaisuuksia sisältävien viestien salaukseen järjestelmää, jossa jokainen kirjain korvattiin aakkosissa siitä kolme merkkiä vasemmalla olevalla kirjaimella. Tieto tästä toimi siis avaimena, jolla salaus voitiin purkaa. Nykyaikainen

[9] Termit tulevat kreikan kielen sanoista *kryptós* (piilossa, salainen) sekä *logia* (oppi) ja *graphein* (kirjoitus).

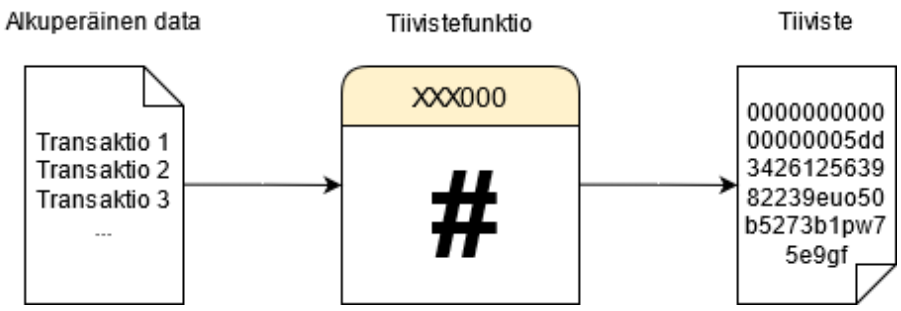
ja tietoteknisesti monimutkainen kryptografia toimii myös hyvin samalla periaatteella avaimineen, ja sen tavoitteena on datan luottamuksellisuuden, varmuuden ja eheyden ylläpitäminen erilaisissa verkkoympäristöissä ja ohjelmistoissa (Johansson ym., 2019, s. 58).

3.2.2 Tiivistefunktio ja tiiviste

Yksi tärkeä osa lohkoketjun kryptografiaa on tiivistefunktiot eli hajautusfunktiot sekä tiivisteet eli hajautusarvot (hash). Tiiviste on matemaattinen arvo, jossa tieto on tiivistetty pienempään kokoon, jotta muun muassa alkuperäisen tiedon yhtenäisyyttä ja muuttumattomuutta voidaan vertailla. Tiivisteitä voidaan hyödyntää etenkin konsensusalgoritmeissa, digitaalisissa allekirjoituksissa ja datan varmentamisessa. Tiivistefunktio voi olla mikä tahansa algoritmi[10] tai funktio, joka laskee annetulle syötteelle (esimerkiksi merkkijono) jonkin hajautusarvon. Tiivistefunktion avulla voidaan suorittaa tiivistäminen (hashing), jossa esimerkiksi jokin tiedosto ajetaan funktiolla ja saatu lopputulos on tiiviste, yleensä lyhyempi merkkijono, jota ei voi enää palauttaa alkuperäiseen muotoonsa. Esimerkiksi jokaisen ihmisen geeniperimä voitaisiin tiivistää 64-merkkiseksi merkkijonoksi, joka toimii ainutlaatuisena ja henkilökohtaisena tunnisteena alkuperäisestä tiedosta. Mikäli tiedon sisältö pitäisi tarkistaa, voidaan sama tiivistefunktio ajaa samalle tiedostolle ja lopputuloksena syntyvä tiiviste pitäisi olla sama kuin aikaisemmin, mikäli tiedosto ei ole muuttunut. Tiivistearvot ovat tarpeeksi lyhyitä, että ne voidaan helposti sisällyttää merkkijonona osaksi dataa lohkoketjussa, mikä mahdollistaa turvallisen aikaleimauksen, josta näkee tarkan todenteen esimerkiksi transaktion tapahtumisajasta.

Kuviossa 2 on esitelty esimerkin avulla alkuperäisen datan muuttaminen tiivistefunktion avulla tiivisteeksi.

[10] Algoritmi on matemaattinen kuvaus tai ohjeistus jonkin tietyn ongelman ratkaisemiseksi.



Kuvio 2: Esimerkki tiivistämisestä.

3.2.3 Julkisen avaimen salaus ja varmenne

Lohkoketjun yksi tärkeimmistä kryptografisista piirteistä on julkisen avaimen salaus eli PKI (public key infrastructure), jota käytetään lohkoketjussa tiedon salaustapana ja digitaalisissa allekirjoituksissa. PKI:n perustana on kahden avaimen, yksityisen ja julkisen avaimen, muodostama pari. Nämä avaimet muodostavat aina parin eli yhtä julkista avainta kohtaan on yksi yksityinen avain ja päinvastoin. PKI:n idea on siinä, että käyttäjä omistaa nämä molemmat avaimet siten, että julkinen avain on kaikkien muiden käyttäjien tiedossa, kun taas yksityinen avain on pidettävä vain käyttäjän omana tietona. Käyttäjä voi näin ollen salata esimerkiksi tiedoston yksityisellä avaimellaan, mutta se voidaan avata vain tähän avaimeen linkitetyllä julkisella avaimella. Julkinen avain voi olla kenen tahansa halussa ja se on julkista tietoa, mutta se voi purkaa salauksen ainoastaan niistä tiedoista, jotka on salattu siihen kytketyllä yksityisellä avaimella. Tämän avulla voidaan olla täysin varmoja siitä, että tiedoston salannut henkilö omistaa myös julkista avainta vastaavan yksityisen avaimen. Näin ollen toimijoiden välinen tiedonsiirto on molemmin puolin suojattua sekä luotettavaa.

Digitaalista varmennetta (digital certificate) voidaan käyttää nimensä mukaisesti todisteena käyttäjien digitaalisen identiteetin varmentamiseksi. Digitaalisten varmenteiden avulla voidaan kryptografisesti yhdistää julkiset avaimet niiden omistajiin sekä jakaa avaimia salausta varten, esimerkiksi digitaalisissa allekirjoituksissa. Näiden varmenteiden taustalla toimii PKI. Digitaalisessa allekirjoituksessa data allekirjoitetaan siitä luodun tiivisteen avulla, mikä sen jälkeen salataan allekirjoittajan yksityisellä avaimella. Allekirjoituksen sisältämä tiiviste

voidaan varmentaa vain allekirjoittajan julkisella avaimella. Tämän jälkeen sama prosessi käydään läpi itse allekirjoitettavassa sisällössä, minkä jälkeen verrataan tiivisteiden yhteneväisyyttä.

3.2.4 Lohkoketjun kryptografiset periaatteet

Salaus itsessään on osa kryptografiaa ja se viittaa prosessiin, jossa viesti tai tieto muutetaan lukukelvottomaksi sekä toisin päin. Näin ollen tiivistefunktiot ja tiivisteet eivät itsessään ole salausta, toisin kuin PKI, sillä tiivistettyä tietoa ei voida enää palauttaa alkuperäiseen muotoonsa. Tiivistefunktiot ovat kuitenkin lohkoketjussa ensisijaisen tärkeitä siinä olevan tiedon eheyden ja muuttumattomuuden tarkistamisessa, mikä liittyy olennaisesti konsensusalgoritmeihin. Lohkoketjun yksi perusajatuksista on ihmisiin ja organisaatioihin kohdistetun luottamuksen korvaaminen matematiikalla. Kaikki lohkoketjut hyödyntävät seuraavaa kolmea kryptografista periaatetta:

1) Jokainen transaktio lohkoketjussa on sen toimeenpanijan digitaalisesti allekirjoittama.
2) Jokainen transaktio – yksittäin tai lohkoissa – on kiinnitetty edelliseen transaktioon digitaalisen tiivisteen avulla.
3) Varmennetut transaktiot tallennetaan jokaiselle laitteelle käyttäen konsensusalgoritmia. (Johansson ym., 2019, s. 131.)

Nämä periaatteet tekevät lohkoketjusta kryptografisen tilikirjan, joka koostuu muuttumattomista merkinnöistä, ja jonka dataa on käytännössä mahdoton muuttaa jälkikäteen tai manipuloida tulevaisuudessa.

3.3 Konsensus

3.3.1 Konsensusongelma

Yksi hajautettuihin järjestelmiin liittyvistä suurimmista haasteista oli pitkään niin sanottu bysanttilaisten kenraalien ongelma (Byzantine generals' problem). Ongelmaa kuvaa hyvin paljon käytetty esimerkki keskiaikaisesta tilanteesta, jossa ryhmä

bysanttilaisia kenraaleja divisioonineen piirittää vihollislinnaa ja valmistautuu valloittamaan sen. Kenraalit ovat maantieteellisesti erillään toisistaan linnan ympärillä ja viestit kulkevat heidän välillään vain lähettien välityksellä, joten tietyllä hetkellä kenraalit eivät tiedä, mitä toiset kenraalit aikovat tehdä. Onnistuakseen vihollislinnan valloituksessa kenraalien on päästävä yhteisymmärrykseen hyökkäyshetkestä, sillä linnan valtaaminen onnistuu ainoastaan, jos kaikki divisioonat hyökkäävät yhtä aikaa. Ongelma syntyy siitä, että kenraalit eivät voi luottaa toisiin kenraaleihin, sillä osa heistä saattaa olla pettureita tai toimia omia etujaan tavoitellen. Lisäksi lähetit saattavat tahallaan välittää eteenpäin väärää tietoa kenraaleille tai jäädä kiinni matkalla. Vain yhdenkin epärehellisen kenraalin tai väärän viestin takia kaikki muut voivat kuolla taistelussa. Keskitetyssä ympäristössä kenraalit välittäisivät hyökkäyssuunnitelmansa luotettavan keskusviranomaisen eli esikunnan kautta, mutta hajautetussa tilanteessa esikuntaa ei ole, joten yhteisymmärryksen saavuttaminen on hankalampaa.

Samoin kuin keskiaikaisessa esimerkissä, lohkoketjun hajautetussa rakenteessa ei ole keskitettyä luotettua keskusviranomaista ja solmut eivät voi luottaa toisiinsa. Ratkaisu ongelmaan on löytää yhteiskäytäntö tai algoritmi, joka varmistaa kenraalien tai solmujen yhteisymmärryksen huolimatta siitä mitä epärehelliset kenraalit tai solmut tekevät. Konsensusalgoritmit ovat ratkaisu lohkoketjun konsensusongelmaan. Käytännössä konsensusalgoritmit varmistavat, mikä tilikirjaan lähetetty tieto, transaktio tai data merkitään säilytettäväksi ja mikä data voidaan hylätä. Avoimissa ja julkisissa lohkoketjuissa mikä tahansa solmu voi liittyä verkkoon sekä lähettää siinä dataa osaksi ketjua, joten alustavasti tässä tilanteessa vallitsee bysanttilaisten kenraalien ongelma. Ainoastaan tietyt yhteiset säännöt, käytännöt ja standardit, jotka ovat koodattu toimintalogiikkoina järjestelmään, voivat pakottaa kaikki verkon toimijat noudattamaan konsensusta. Tätä kutsutaan konsensusprotokollaksi. Mikäli protokollaa noudatetaan transaktioita suoritettaessa, verkon muut solmut hyväksyvät siinä lähetetyn datan, ja päinvastaisessa tilanteessa data voidaan hylätä.

3.3.2 Konsensusalgoritmit

Konsensusalgoritmit ovat matematiikkaan perustuvia mekanismeja, joilla konsensusprotokollan mukainen yhteisymmärrys saavutetaan. Hajautetussa verkossa toimiessaan lohkoketjun jokaisella käyttäjällä on identtinen kopio ketjun sisältämästä

datasta, joten tässä tapauksessa käyttäjien poistuminen verkosta ei vaikuta tiedon säilymiseen. Konsensusalgoritmit takaavat tiedon säilymisen ja yhtenäisyyden, kirjaamisjärjestyksen sekä verkon toimijoille saman kuvan lohkoketjun tiedoista. Algoritmit takaavat nämä asiat matemaattisesti todistettavalla tavalla, joten luottamusta yksittäisiin verkon toimijoihin ei tarvita. Käytettyjä konsensusalgoritmeja ovat muun muassa Proof-of-Work-algoritmi (PoW), bysanttilainen häiriötoleranssi -algoritmi (BFT) ja Proof-of-Stake-algoritmi (PoS) (Johansson ym., 2019, s. 62–63). Esimerkiksi bitcoin käyttää toiminnassaan PoW:ia, joka yksinkertaistettuna perustuu verkon toimijoiden suorittaman laskennan määrään sidottuna siihen käytettyyn aikaan. Tämän avulla päästään konsensukseen siitä, mitkä transaktiot lisätään missäkin järjestyksessä tilikirjaan. Käytännössä PoW tunnistaa verkon epärehelliset toimijat tiivistefunktion avulla luotujen tiivisteiden avulla. Jos epärehellinen toimija yrittää bitcoin-lohkoketjussa käyttää samaa yksittäistä virtuaalivaluuttayksikköä useammin kuin kerran[11], PoW tunnistaa epärehellisen toiminnan transaktioon liitetystä tiivisteestä, joka on todiste alkuperäisen transaktion oikeellisuudesta. Alkuperäisen datan muuttuminen näkyy täysin erilaisesta tiivisteestä, sillä pienikin muutos alkuperäiseen dataan vaikuttaa tiivistefunktion avulla muodostettuun tiivisteeseen.

Proof of work kuvaa nimensä mukaisesti sitä, että tiettyä dataa kohti on suoritettu tarpeeksi työtä eli ratkaistu laskennallisia ongelmia. Esimerkiksi PoW:ssa solmu laskee monimutkaisten matemaattisten ongelmien kautta sattumanvaraisia tiivisteitä lohkolle. Kun oikea tiiviste on löytynyt jonkin verkon solmun toimesta, lohko varmistetaan ja se lisätään osaksi ketjua. Lohkoketju voi käyttää omaa lanseeraamansa virtuaalivaluutta vaivanpalkkana tästä tehdystä laskentatyöstä, jonka avulla verkon konsensusta transaktioiden oikeellisuudesta ylläpidetään. Tätä koko prosessia kutsutaan louhimiseksi. Virtuaalivaluutan louhinta tarkoittaa siis käytännössä prosessia, jossa verkon solmu toteuttaa tiettyä konsensusalgoritmia ja saa siitä vastineeksi uusia virtuaalivaluuttayksiköitä. Esimerkiksi bitcoinin (2021) protokollan mukaan olemassa tulee olemaan kaiken kaikkiaan vain 21 miljardia bitcoinia, minkä vuoksi lohkon louhimisesta saatava lohkopalkkio puoliintuu noin joka 210 000 lohkon välein. Alun perin lohkopalkkio oli 50 bitcoinia, mutta nykyään se on neljän

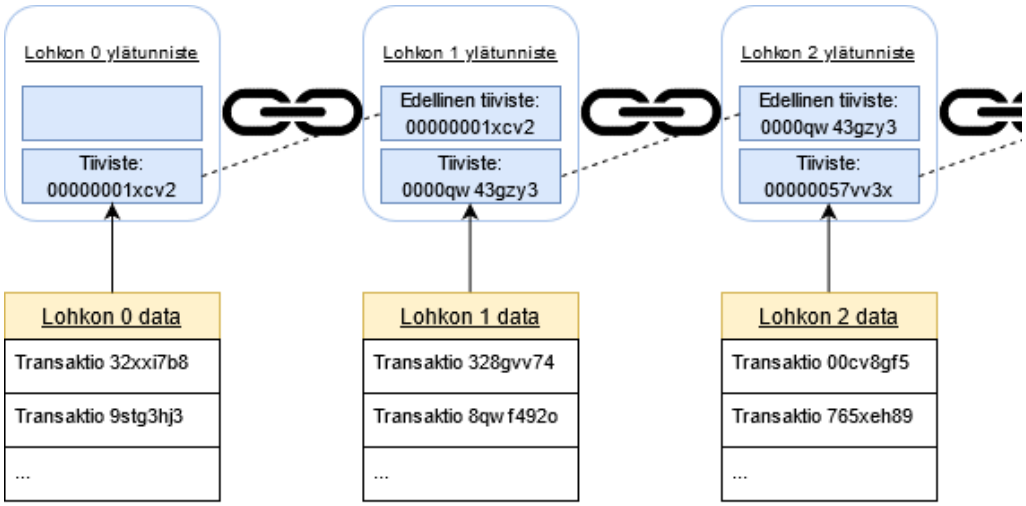
[11] Tätä kutsutaan *kaksinkertaisen käytön ongelmaksi*.

puolittumisen jälkeen 6,25 bitcoinia. Sen sijaan lohkoketjuympäristö Ethereumin käyttämän PoS:in tapauksessa tämä laskennallinen työ on korvattu omistusoikeudella lohkoketjusta, esimerkiksi jostain virtuaalivaluutasta. Mitä enemmän käyttäjä omistaa PoS:ia hyödyntävästä lohkoketjusta, sitä enemmän tämä voi louhia lohkoja ja luoda sitä kautta lisää virtuaalivaluuttayksiköitä.

3.4 Lohko ja ketju

Lohko on lohkoketjun perusosa, joka sisältää tietyn määrän dataa tai transaktioita. Lohko voidaan ajatella ikään kuin yhtenä sivuna tilikirjassa, ja kun se tulee täyteen dataa, saa se jatkokseen uuden lohkon. Lohkon sisäiset tiedot salataan PKI:tä hyödyntävien digitaalisten allekirjoitusten avulla ja ne yhdistetään toisiinsa tiivisteiden avulla. Lohkoketjun ensimmäistä lohkoa kutsutaan luomislohkoksi (genesis block), josta alkaa katkeamaton ketju seuraaviin lohkoihin. Varsinaista ketjua sanan merkityksessä ei lohkojen välillä ole, vaan lohkot yhdistyvät toisiinsa tiivisteiden avulla. Jokainen lohko sisältää edeltäneen lohkon oman tiivisteen, ja tätä kautta syntyy tavallaan ketju lohkojen välille. Kaikki lohkojen sisältämät tiedot on varmennettu digitaalisten allekirjoitusten ja tiivisteiden avulla, joten lohkoketjussa on selkeä käsitys tietojen tai transaktioiden kronologisesta järjestyksestä ja oikeellisuudesta. Tämän takia jo varmennetut lohkot ovat menneisyyttä ja pysyvä osa ketjua, eikä niitä voi enää jälkikäteen muokata.

Kuvio 3 on havainnollistava ja karkea esimerkki lohkojen ketjuttamisesta toisiinsa tiivisteiden avulla. Jokainen lohko sisältää datan, joka voi olla esimerkiksi lista transaktioita, jotka on varmennettu kryptografisesti.



Kuvio 3: Lohkoketjun muodostuminen.

4 LOHKOKETJUTEKNOLOGIAN OMINAISUUDET

Lohkoketju on itsessään uusi teknologia, mutta sen pienempiä osia ja siinä hyödynnettyjä teknologioita on käytetty jo kauemmin. Tämän takia lohkoketju kohtaa sekä vanhoja että täysin uusia haasteita sen toimivuuden ja toteutuksen kannalta. Toisaalta osalle ongelmista löytyy uusia ratkaisuja teknologian kehittyessä jatkuvasti. Lisäksi lohkoketju hyötyy erilaisista mahdollisuuksia, jotka erottavat sen muista kilpailevista teknologioista. Tässä luvussa käsitellään eri haasteita ja heikkouksia sekä mahdollisuuksia ja vahvuuksia, joita lohkoketjuteknologiaan liittyy.

4.1 Hajautetun järjestelmän ominaisuudet

Tässä tutkielmassa on korostettu paljon lohkoketjun hajautukseen liittyviä ominaisuuksia: lohkoketju on hajautettu julkinen tilikirja tai tapahtumarekisteri, joka toimii hajautettuna tietokantana vertaisverkossa. Nakamoto (2008) korosti jo white paper -julkaisussaan bitcoinin ja lohkoketjun perusajatuksen nojaavan vertaiselta vertaiselle käytäviin transaktioihin ilman luotettua kolmatta osapuolta. Tämän takia on luontevaa tarkastella aluksi lohkoketjun ominaisuuksia hajautettuna järjestelmänä.

Mikäli lohkoketju nähdään perustavanlaatuisena teknologiana, ehkä paras esimerkki ja käyttötapaus, mihin sitä voidaan verrata, on TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP on useamman tietoliikenneprotokollan yhdistelmä eli pino, ja se toteuttaa Internet-arkkitehtuurin. Se kehiteltiin vuonna 1972 ja se toimi pohjana tutkijoiden väliselle sähköpostiviestinnälle Yhdysvaltain puolustusministeriön ARPANETissä, josta kehittyi myöhemmin kaupallinen internet. Ennen TCP/IP:tä televiestintäarkkitehtuurit pohjautuivat piirikytkennälle[12], jossa kahden osapuolen välinen yhteys piti olla jatkuvasti avoinna ja ennalta määrätty koko yhteystapahtuman ajan. TCP/IP sen sijaan lähettää tietoa muuttamalla sen digitaaliseksi ja pilkkomalla sen verkkopaketteihin, jotka kaikki sisältävät lähetysosoitteet. Verkkopaketit voivat kulkea vastaanottajalle verkossa mitä tahansa reittiä pitkin, ja verkon reunamilla toimivat vastaanottavat sekä lähettävät älykkäät

[12] Esimerkki piirikytkentää hyödyntävästä televiestintäverkosta on perinteinen puhelinverkko.

solmut purkavat ja kokoavat verkkopaketteja tulkitakseen koodattua dataa. TCP/IP:n tapauksessa ei näin ollen tarvittu omia virtapiirejä tai suurta infrastruktuuria ja se loi avoimen ja hajautetun tietoverkon ilman yksittäistä keskusviranomaista tai ylläpitäjää. TCP/IP kohtasi aluksi paljon skeptisyyttä perinteisiltä televiestinnän ja tietojenkäsittelytieteen sektoreilta, mutta se popularisoitui viimein 1980-luvun vaihteessa ja 1990-luvulla. Useat yritykset, kuten Sun, NeXT, Hewlett-Packard ja Silicon Graphics käyttivät TCP/IP:tä paikallisten yksityisten tietoverkkojen rakentamiseen organisaatioiden sisällä. Tämä johti TCP/IP:n käyttötarkoituksien laajenemisen sähköpostiviesteistä eteenpäin ja vähitellen uudet työkalut syrjäyttivät vanhat teknologiat sekä toimintatavat. Yritykset kokivat uuden teknologian omaksumisesta suurta kasvua tuottavuudessaan ja lopulta TCP/IP tuli julkiseen käyttöön World Wide Webin myötä 1990-luvun puolessavälissä. (Iansiti & Lakhani, 2017.) Tämän myötä käytännössä kaikki palvelut siirtyivät vähitellen internetiin uuden kustannustehokkaan tietoliikenneprotokollan houkuttelemana.

Usein internetistä puhutaan neljännen teollisen vallankumouksen käynnistäneenä perustavanlaatuisena teknologiana, mutta todellisuudessa sen täyden potentiaalin valjasti TCP/IP. Tästä huolimatta internetillä sekä TCP/IP:llä kesti yli 30 vuotta kulkea koko yhteisen kehityskaarensa läpi ja vakiinnuttaa asemansa koko talousjärjestelmän muuttajina. Yhteneväisyydet TCP/IP:n ja lohkoketjun välillä ovat huomattavat. Aivan kuten TCP/IP mahdollisti sähköpostit ja kahdensuuntaisen viestinnän käyttäjien välillä, lohkoketju mahdollisti bitcoinin ja kahdensuuntaisen virtuaalivaluuttatransaktion käyttäjien välillä. Bitcoin on vain jäävuoren huippu siitä, mitä lohkoketjulla voi tehdä. Sekä TCP/IP että lohkoketju perustuivat ajatukselle avoimuudesta, hajautuksesta ja jakamisesta, mutta esimerkiksi internet on lopulta kehittynyt hyvin keskitetyksi järjestelmäksi. Lohkoketju voi myös kehittyä samaan suuntaan, erityisesti tiukasti keskitettyjen ja yksityisten lohkoketjujen kautta, mikä ei enää edustaisi lohkoketjun perusajatusta läpinäkyvyydestä.

Internetin kaupallistuminen esimerkiksi Facebookin, Googlen, Twitterin ja Snapchatin kaltaisten palveluntarjoajien tulon myötä on johtanut internetin keskittymiseen. Näiltä alustoilta kerättyä käyttäjätietoa on ryhdytty käyttämään hyödykkeenä, jota myydään muun muassa mainostoimistoille, markkinointiyrityksille ja tutkimusryhmille. Tällöin informaatio ei ole vapaata tai ilmaista ja ongelmia syntyy varsinkin silloin, jos nämä

tiedot ajautuvat pahantahtoisten toimijoiden käsiin. Tiedon keskittyminen suurten yritysten palvelimille ja tietokantoihin altistaa ne hakkereille ja DDOS-palvelunestohyökkäyksille. Suuret yritykset ovat edelleen hyvin haavoittuvaisia kyberrikollisille ja hyökkäyksille, mikä ei ole juurikaan ongelma hajautetussa järjestelmässä.

Lohkoketjun hajautukseen liittyvä keskeinen hyöty on luottamuksen korvaaminen digitaalisilla allekirjoituksilla ja konsensusalgoritmien kautta tehdyillä varmennuksilla. Keskitetty viranomainen eli luotettu kolmas osapuoli on aina altis käyttäjien tietojen menettämiselle esimerkiksi hyökkäysten tai tietojen myymisen seurauksesta. Tämä heikentää käyttäjien luottamusta yrityksiä ja muita organisaatioita kohtaan entisestään. Sen sijaan hyvin hajautetussa järjestelmässä luottamus voitaisiin poistaa kokonaan. Lisäksi hajautettu järjestelmä ei ole altis yksittäisille hyökkäyspisteille, jotka voivat vaikeuttaa muunkin verkon toimintaa. Esimerkiksi keskitetyn tunnistepalvelun kaatuessa käyttäjä ei voi myöskään käyttää siihen linkittyneitä muita verkkosivuja tai palveluita. Hajautetussa tietoverkossa tietoliikenteen sensuroiminen on myös paljon vaikeampaa, sillä siinä lähetetty data kommunikoi automaattisesti solmujen kanssa, jotka voivat taas lähettää dataa eteenpäin. Näin valtiot tai yritykset eivät voi määrätä esimerkiksi internet-palveluntarjoajaa estämään tietoliikennettä yhden yrityksen palvelimelle ja rajoittaa kokonaan pääsyä yrityksen sivuille. Lisäksi hajautettu verkko tarjoaa avoimen järjestelmän, jota kuka tahansa voi kehittää muun muassa palveluiden, tuotteiden ja työkalujen muodossa. (Johansson ym., 2019, s. 246–247.)

4.2 Julkiset ja yksityiset lohkoketjut

On olemassa sekä julkisia että yksityisiä lohkoketjuja. Molemmat toimivat hajautetussa vertaisverkossa, jossa jokaisella toimijalla on oma kopionsa digitaalisesti allekirjoitettuja transaktioita sisältävästä tilikirjasta. Tässä tutkielmassa esitellyt lohkoketjun tekniset rakenteet myös pätevät molemmissa, kuten vaikkapa verkon yhteisymmärryksen takaavan konsensusprotokollan olemassaolo. Sen sijaan suurin ero julkisten ja yksityisten lohkoketjujen välillä on kysymys siitä, kuka saa ylläpitää jaettua tilikirjaa, liittyä osaksi verkkoon ja osallistua konsensusprotokollaan toteuttamiseen (Johansson ym., 2019, s. 76).

Julkiset lohkoketjut ovat avoimia kaikille, kuka tahansa voi liittyä verkkoon sekä osallistua avoimesti datan lisäämisen osaksi lohkoketjua. Tässä tapauksessa lohkoketjun hallinta ei ole keskitettyä, minkä vuoksi tietoja ei voida digitaalisten varmennusten jälkeen enää muuttaa tai poistaa. Julkisissa lohkoketjuissa konsensuksen ylläpitämiseen tarvitaan erilaisia konsensusalgoritmeja, kuten PoW tai PoS, jotka vaativat verkon solmuilta esimerkiksi laskentatyötä tai omistusosuutta verkosta transaktioiden varmentamiseksi. Konsensusalgoritmeja toteuttavat solmut ylläpitävät näin ollen verkkoa, ja saavat tästä vaivanpalkaksi esimerkiksi lohkoketjun omaa virtuaalivaluuttaa. Tästä aiheutuu julkisen lohkoketjun eräs haaste eli suuren laskentatehon ja energian kuluminen lohkoketjun ylläpitämiseen, etenkin PoW:in tapauksessa. Tällä hetkellä esimerkiksi Visa (2021a) päihittää transaktioiden prosessoimisessa selkeästi julkiset lohkoketjut. Toinen merkittävä julkisten lohkoketjujen haaste liittyy transaktioiden läpinäkyvyyteen. Kaikille julkiset transaktiot voivat johtaa erityisesti yritysmaailmassa epäsymmetriseen tietoon ja epäreiluihin kilpailuetuihin, mikäli jokin osapuoli saisi selville toisen osapuolen identiteetin lohkoketjussa.

Yksityisessä lohkoketjussa toimijoiden pääsyä verkkoon rajoitetaan eli verkko on niin sanotusti suljettu. Yleensä yksityisen lohkoketjun konsensusprotokollaan on asetettu rajoitukset siitä, kuka saa osallistua verkkoon, minkälaisia transaktioita saadaan suorittaa ja mihin tietoihin toimijoilla on pääsy. Osaksi tällaista suljettua verkkoa voi päästä esimerkiksi nykyisten käyttäjien lähettämän kutsun, identiteetin varmistamisen tai keskusviranomaisen myöntämän lisenssin kautta. Yksityisen lohkoketjun hyviä puolia ovat esimerkiksi käyttäjien digitaalisen identiteetin helpompi tunnistaminen, joka vähentää epärehellisyyttä verkossa, sekä transaktioiden osapuolten identiteettien piilottaminen muilta kuin kyseisiltä osapuolilta. (Johansson ym., 2019, s. 77.) Lisäksi yksityisten lohkoketjujen konsensuksen takaamiseksi ei vaadita esimerkiksi paljon laskentatehoa kuluttavia konsensusalgoritmeja, joten julkisiin lohkoketjuihin verrattuna yksityisissä lohkoketjuissa saavutetaan parempi skaalautuvuus transaktioissa. Edellä mainittujen ominaisuuksiensa vuoksi yksityiset lohkoketjut ovat houkuttelevia etenkin pankkien ja rahoituslaitoksien käyttöön, ja ne voivatkin tulevaisuudessa syrjäyttää instituutioiden nykyiset sisäiset verkkojärjestelmät.

4.3 Tekniset haasteet ja ratkaisut

Vaikka monet konsensusalgoritmit (kuten PoW) ratkaisevat bysanttilaisten kenraalien ongelman, on silti mahdollista, että kaksi lohkoa liittyvät osaksi ketjua yhtä aikaa, synnyttäen niin sanotun *haarukan* eli lohkoketjun haarauman. PoW:ia käyttävä bitcoinin lohkoketju ratkaisee tämän konsensusongelman varmentamalla lohkon osaksi ketjua vasta kun sen jälkeen on lisätty jokin tietty määrä lohkoja (yleisesti kuusi). Tämä toimenpide aiheuttaa taas ongelmia tietoturvaan ja suorituskykyyn, sillä hetkellisen konsensuksen puutteen vuoksi suuri osa lohkoketjun solmuista voi päätyä epärehellisten toimijoiden käsiin, pahimmassa tapauksessa halliten koko verkkoa 51 prosentin enemmistöomistuksella. Tällainen tilanne antaa mahdollisuuden yhdelle toimijalle hallita koko verkkoa, mutta tietyissä konsensusalgoritmeissa tämä on käytännössä mahdotonta. (Dinh ym., 2018.) Useimmat julkisista lohkoketjuista käyttävät PoW:in ja PoS:in kaltaisia konsensusalgoritmeja yhteisymmärryksen saavuttamiseksi, mutta ne toimivat huonosti yksityisissä lohkoketjuissa varsinkin niiden sähköä kuluttavan laskentatehon ja matalan skaalautuvuuden takia.

PoW:iin kuluvan laskentatehon takia myös yleisesti lohkoketjuteknologiaa kohtaan on kohdistettu kritiikkiä runsaasta sähkönkulutuksesta. Monimutkaisten funktioiden laskeminen sopivan tiivisteen löytämiseksi vaatii solmuilta todella paljon laskentatehoa ja sitä kautta myös sähköä. Bitcoinin sähkönkulutusta seuraava internetsivusto digiconomist.net on laskenut PoW:ia käyttävän bitcoin kuluttavan yhdessä transaktiossa yhdysvaltalaisen kotitalouden keskimääräisen 37,13 päivän kulutuksen verran sähköä vuonna 2021 (de Vries, 2021). Vaikka bitcoin toimiikin PoW-konsensusalgoritmin avulla, läheskään kaikki lohkoketjut eivät toimi samalla periaatteella. PoS luotiin alun perin vastaukseksi PoW:in sähkönkulutusongelmaan, mutta toistaiseksi sitä käyttävät pääsääntöisesti vain virtuaalivaluutat. PoS:issa laskentatyö korvataan vastaavalla omistusoikeudella lohkoketjusta, joten sähkönkulutus on huomattavasti vähäisempää. Tämä ajatus tarjoaa myös ratkaisun bitcoinin PoW:ia uhkaavaan yhteismaan ongelmaan, jossa jatkuvasti puolittuva lohkopalkkio vähentää konsensusprotokollaa ylläpitävien louhijoiden määrää. Konsensusta ylläpitävien solmujen pienentyvä määrä altistaa PoW:illa toimivan lohkoketjun myös aikaisemmin mainitulle 51 prosentin hyökkäykselle, jossa jokin taho voi hallita koko verkkoa ja käyttää sitä epärehellisiin tarkoituksiin. PoS:issa tämä

on käytännössä lähes mahdotonta, sillä tehokkaampi louhintateho vaatii käyttäjältä suuremman omistusosuuden lohkoketjusta (kuten virtuaalivaluutasta). Tämä on itsessään omistusta hajauttava ja itseään ruokkiva prosessi, sillä siinä syntyy jatkuvasti uutta arvoa.

Sähkönkulutukseen ja ympäristöystävällisyyteen liittyvät ongelmat nostetaan hyvin usein esille lohkoketjuteknologiasta puhuttaessa, mutta oikeastaan ne ovat vain tiettyjä lohkoketjuja koskevia ongelmia, erityisesti niissä käytettävien konsensusalgoritmien ja -protokollien takia. Lohkoketjun toiminnan parantamiseksi keksitään jatkuvasti uusia konsensusalgoritmeja, jotka soveltuvat eri käyttötarkoituksiin. PoW:n ja PoS:n rinnalle on tullut esimerkiksi Proof-of-Authentication (PoAh), joka yhdistää kahden edellä mainitun ajatukset aktiivisesta laskennasta sekä omistusosuudesta kevennettyyn tiivistefunktioon (Puthal & Mohanty, 2019). Lisäksi PoS:ia kehitellään jatkuvasti eteenpäin ja PoW:in korvaajaksi on kaavailtu Proof-of-Conceptia (PoX), joka korvaa tiivisteiden satunnaisen etsimisen päämäärätietoisella laskennalla ja parantaa suorituskykyä etenkin tietoturvan, kannustimien ja resurssinkäytön saralla (Nguyen ym., 2019).

Yksi usein mainittu kritiikki lohkoketjuteknologiaa kohtaan on sen huono suorituskyky ja transaktioiden skaalautuvuus verrattuna esimerkiksi pankkien tai luottolaitosten nykyisiin järjestelmiin. Julkisista lohkoketjuista bitcoin prosessoi noin seitsemän transaktiota sekunnissa ja älykkäitä sopimuksia varten kehitetty Ethereum noin 25 transaktiota sekunnissa (Johansson ym., 2019, s. 219). Lohkoketjussa matala skaalautuvuus johtuu usein lohkojen pidemmästä varmentamisajasta, etenkin ketjun haarukoiden välttämiseksi. IBM:n vuonna 2010 suorittaman testin mukaan Visan (2021a) maksujärjestelmä Visanet kykenee prosessoimaan noin 24000 transaktiota sekunnissa, mutta todellisuudessa prosessoidut transaktiot ovat keskimäärin noin 1700 sekunnissa. Yleisesti mitä keskitetympi lohkoketju on, sitä vähemmän konsensuksen saavuttamiseen vaaditaan, joten monet keskitetyt lohkoketjut kykenevät prosessoimaan huomattavasti enemmän transaktiota sekunnissa kuin vahvasti hajautetut lohkoketjut. Algoritmien kehittyessä lohkoketjujen skaalautuvuus myös paranee, joten onkin tarpeen pohtia, missä lohkoketjun käyttötarkoituksessa hyvä skaalautuvuus edes on tarvittavaa. Esimerkiksi asunto-osakkeiden kaupankäynnin suoritus nykyisellään kestää päivä tai viikkoja, mutta lohkoketjuteknologian avulla

tämä aika voi pienentyä tuntiin (Johansson ym., 2019, s. 220). Huomioitavaa on, että 29. maaliskuuta 2021 Visa (2021b) ilmoitti hyväksyvänsä USD Coin -johdannaisvirtuaalivaluutan (stablecoin)[13] käytettäväksi valuutaksi maksujärjestelmässään. Tämä on merkittävä kehitysaskel lohkoketjuteknologian laajemmassa omaksumisessa, sillä se osoittaa skaalautuvuusongelman merkityksen pienentymisen, kun teknologia kehittyy kokonaisvaltaisesti.

4.4 Maine, asenteet ja osaaminen

Lohkoketjun laajemman omaksumisen tiellä ovat toistaiseksi myös ihmisten asenteet ja suhtautumiset etenkin virtuaalivaluuttoihin yleisesti sekä niiden avulla harjoitettuun rikolliseen toimintaan. Vaikka virtuaalivaluutat ovat vain yksi lohkoketjun käyttökohde, monet ihmiset pitävät näitä kahta asiaa toistensa synonyymeina. Lohkoketjuteknologia ja virtuaalivaluutat itsessään ovat puolueettomia teknologioita, joita voidaan luonnollisesti käyttää sekä hyvään että pahaan tarkoitukseen, aivan kuten tavallista rahaakin. Toisaalta virtuaalivaluuttojen avulla rahoitettu rahanpesu, huumekauppa ja muut laittomat toimet voivat aiheuttaa sille vastareaktion uuden teknologian muodossa, aivan kuten aikoinaan tietokonevirukset synnyttivät virustentorjuntasovellukset. Lisäksi huolta ihmisissä aiheuttaa erinäisten vaihtoehtoisten kryptovaluuttojen pump and dump -huijaukset, joissa valuutan hintaa manipuloidaan keinotekoisesti nostamalla sitä ja sitten myymällä ylihintaisena pois aiheuttaen kurssin romahduksen (Swan, 2015, s. 88). Ainoa selvä ratkaisu lohkoketjun maineen parantamiseksi onkin sen laajempi omaksuminen ja liiketoimintamallien kehittyminen. Lisäksi uutena teknologiana lohkoketju tarvitsee luonnollisesti paljon osaajia, kuten ohjelmoijia, jotta se voitaisiin omaksua ja toteuttaa laajemmin. Tällä hetkellä osaajien puute, mutta myös yleinen tietämättömyys lohkoketjuteknologian ominaisuuksista on huomioitava tekijä sen tulevaisuuden näkymiä arvioitaessa.

[13] Stablecoin on virtuaalivaluutta, jonka arvo on sidottu johonkin toiseen kohde-etuuteen, kuten toiseen virtuaalivaluuttaan, rahaan tai arvometalliin. USD Coin eli USDC on sidottu Yhdysvaltojen dollarin arvoon.

4.5 Lainsäädäntö ja sääntely

4.5.1 Sääntely

Toistaiseksi lohkoketjuteknologia ei ole kohdannut suurempia lainsäädännöllisiä rajoitteita, mutta nopeasti kehittyvän teknologian tapauksessa on aina olemassa riski siihen, että lainsäädäntö ei ehdi kehittyä sen perässä. Tällä hetkellä lohkoketjuteknologiaa koskevaa sääntelyä ei ole Suomessa. Virtuaalivaluuttojen kanssa on ollut paljon epävarmuutta etenkin verotukseen liittyen Suomessa, eikä aikaisemmin ollut täyttä selvyyttä siitä, mitä sääntöjä varsinkin virtuaalivaluutoiden luovutusvoitoissa tulisi soveltaa. Kuitenkin korkeimman hallinto-oikeuden 23.9.2019 antaman vuosikirjapäätöksen (KHO 2019:42) mukaan virtuaalivaluuttojen välisessä vaihdannassa syntyneissä voitoissa sovelletaan tuloverolain luovutusvoittoa koskevia säädöksiä (TVL 2:45.1 §; TVL 2:46.1 §), mukaan lukien luovutustappioiden vähentäminen (TVL 2:50.1 §) ja pienten luovutusvoittojen verovapaus (TVL 2:48.6 §). Tällä hetkellä virtuaalivaluuttaa pidetään saman korkeimman hallinto-oikeuden päätöksen (KHO 2019:42) mukaisesti omaisuutena, mutta se ei kuitenkaan ole arvopaperi. Virtuaalivaluuttaa ei myöskään rinnasteta verotuksessa virallisiin valuuttoihin tai muihin maksuvälineisiin. (TVL 2:45.1 §.)

Lainsäädännöllisen epäselvyyden ratkaisemiseksi lohkoketjuihin ja virtuaalivaluuttoihin ei ehkä olisi tarpeen säätää niitä koskevaa erityistä sääntelyä, vaan soveltaa jo olemassa olevaa lainsäädäntöä. Yhdysvalloissa keskustelua on erityisesti herättänyt virtuaalivaluuttojen määrittely joko omaisuuseriksi, arvopapereiksi tai muuksi rahoitusinstrumenteiksi. Yhdysvaltain rahoitusmarkkinoita valvova arvopaperi- ja pörssikomissio SEC:n (United States Securities and Exchange Commission) entinen johtaja Jay Clayton on linjannut CNBC:n (Rooney, 2018) haastattelussa monet digitaaliset poletit (token) ensisijaisesti arvopapereiksi, mutta sen sijaan bitcoinin valuuttaan verrattavissa olevaksi omaisuudeksi, joka ei tulisi kohtaamaan arvopapereita koskevaa sääntelyä. Kommentti on hieman epäjohdonmukainen, mutta yleisesti ottaen SEC ei katso virtuaalivaluuttoja arvopapereiksi. Lainsäädännöllisesti olisi helppo ratkaisu kategorisoida ne joko arvopapereiksi tai omaisuuseriksi. Eri virtuaalivaluutat ja digitaaliset poletit eroavat

kuitenkin toimintatavoiltaan sekä käyttötarkoituksiltaan niin merkittävästi, että niiden niputtaminen yhteen ei ole kestävä ratkaisu.

4.5.2 Yleinen tietosuoja-asetus GDPR

Euroopan unionin yleistä tietosuoja-asetusta ((EU) 2016/679) eli GDPR:ää (General Data Protection Regulation) alettiin soveltamaan EU-maissa 25.5.2018 alkaen. GDPR:n tavoitteena on parantaa EU-kansalaisten henkilötietojen käsittelyn suojaa sekä niiden vapaata liikkuvuutta. GDPR asettaa ihmisille parempia oikeuksia päästä käsiksi dataan, jota eri yritykset, valtiot, palvelut ja yhteisöt heistä jatkuvasti keräävät. Tähän kuuluu oikeus tietää, mitä dataa heistä säilötään ja mihin tarkoitukseen. Lisäksi ihmisillä tulee olla mahdollisuus korjata virheellisiä tietoja, rajoittaa tietojenkäsittelyä ja viime kädessä poistaa tietoja. Suurin ristiriita GDPR:n ja lohkoketjun toiminnan välillä koskee tietojen poistamista, vaikka muuten lohkoketjuteknologia täyttää nykyisellään GDPR:n vaatimukset. Lohkoketjun toimintaperiaatteen mukaisesti lohkoihin tallennettuja tietoja ei voi enää jälkikäteen poistaa, vaan uutta tietoa voidaan ainoastaan lisätä ketjuun. Esimerkiksi lohkoketjuun tallennettuja henkilötietoja voidaan ainoastaan päivittää, mutta ei poistaa. Tämä voi mahdollisesti antaa lohkoketjun kehittämisessä etulyöntiaseman vapaamman sääntelyn maille, kuten USA:lle ja Kiinalle (Johansson ym., 2019, s. 240).

Tietosuoja-asetuksen aiheuttamalle ongelmalle on kuitenkin Johanssonin ym. (2019, s. 240) mukaan löydetty ratkaisu perinteisistä tietokannoista. Käytännössä tämä tarkoittaisi kahden kerroksen järjestelmäarkkitehtuurin rakentamista, missä varsinaiset henkilötiedot tallennetaan perinteisiin tietokantoihin ja tiedoista tehdyt salatut viitteet itse lohkoketjuun. Näin lohkoketjussa käsiteltäisiin vain viitteitä ja varsinaiset henkilötiedot olisivat poistettavissa perinteisistä tietokannoista. Mikäli toimija haluaisi päästä oikeisiin tietoihin käsiksi, tiedon haltija voi pyytää suostumuksen, jonka toimija allekirjoittaa digitaalisesti. Allekirjoituksen sisältämä viesti ohjaisi toimijan lohkoketjun kautta oikean tiedon luokse, missä toimija voisi vapaasti muokata tietojaan GDPR:n mukaisesti. Kahden kerroksen järjestelmäarkkitehtuuri saattaa kuulostaa monimutkaiselta, mutta toisaalta tässä asiayhteydessä monimutkaisuus parantaa yksityisyyden suojaa ja mahdollistaa lohkoketjun monipuolisuuden soveltamisen. Sen sijaan vapaamman lainsäätelyn maat voisivat saada tästä

kilpailuetua lohkoketjuteknologian kehitystyössä ja vastaavasti EU-maissa kehitys saattaisi hidastua. Tämän ei kuitenkaan tule antaa vaikuttaa lohkoketjun kehitykseen negatiivisesti, sillä laajempi lohkoketjun omaksuminen ja rahoittaminen kehittää EU:n sisämarkkinoita itsessään, ja auttaisi muovaamaan nykyistä lainsäädäntöä yhteensopivammaksi.

4.6 Älykkäät sopimukset

Yksi merkittävimmistä lohkoketjuteknologiaan liittyvistä mahdollisuuksista ja ominaisuuksista ovat älykkäät sopimukset. Kryptografi Nick Szabo kehitti ensimmäiset varsinaiset älykkäät sopimukset 1990-luvun alkupuolella, ja ne perustuivat ajatukselle koodilla kirjoitetusta sopimuksesta, joka toteuttaisi sen sisältämiä ehtoja ja lausekkeita automaattisesti tiettyjen reunaedellytysten täyttyessä. Lohkoketjun tapauksessa älykkäitä sopimuksia voi tallentaa sekä hallita lohkoketjun hajautetussa järjestelmässä (Johansson ym., 2019, s. 97–98; Lauslahti, Mattila & Seppälä, 2016; Swan, 2015, s. 16). Ensimmäiset älykkäät sopimukset tulivat konkreettisesti käyttöön kuitenkin vasta lohkoketjuympäristö Ethereumissa vuonna 2015 (Swan, 2015, s. 21). Lohkoketjuteknologian periaate tiedon muuttumattomuudesta tarjoaa älykkäille sopimuksille toimivan alustan, sillä tietokoneohjelmaksi tallennetut sopimusehdot ja eri osapuolten tahdonilmaisut ovat yleisesti alttiita tiedon manipuloinnille jälkikäteen. Älykkäissä sopimuksissa keskusviranomaisia tai välikäsiä ei tarvita, joten niiden käyttöönotossa säästetään välikäsiin menevissä kustannuksissa, kuten paperityössä. Sopimusten läpinäkyvyys ja digitaalisuus takaavat sen, että sopimusten avulla voidaan vaihtaa arvoeriä nopeammin ja sovinnollisemmin. (Johansson ym., 2019, s. 64.)

Älykäs sopimus yhdistää klassisen sopimuskielen sekä ohjelmointikielen eli se voi olla kirjoitettu täysin koodina, luonnollisella kielellä tai jollain siltä väliltä. Yleisesti käytetty vertaus älykkäistä sopimuksista on karkkiautomaatti, johon käyttäjä syöttää rahaa. Tämän jälkeen koneen sisältämä automaatio ratkaisee sopimuksen kaupasta ja lopuksi vapauttaa halutun tuotteen automaatin kouruun. (Johansson ym., 2019, s. 97–98; Lauslahti ym., 2016; Swan, 2015, s. 16–17.) Älykkäät sopimukset laajentavat karkkiautomaatin toimintatavan koskettamaan kaikkia digitaalisesti hallittavia arvoeriä. Sopimukset on usein kirjoitettu ihmisten tekemällä koodilla, joten ne ovat

myös alttiita virheille. Tällä hetkellä älykkäiden sopimusten käyttötarkoitukset rajoittuvat lähinnä transaktioiden automatisointiin, ja laajemman omaksumisen tiellä on erityisesti niihin liittyvän osaamisen puute. Potentiaali tosin on todella suuri, ja onkin kaavailtu, että tulevaisuudessa kokonaiset hallinnot, yhteisöt ja valtiot voisivat olla älykkäiden sopimusten avulla automatisoituja. (Johansson ym., 2019, s. 98.)

5 LOHKOKETJUTEKNOLOGIA RAHOITUSPALVELUISSA

Lohkoketjuteknologia kehitettiin alun perin bitcoinia varten, joten luonnollisesti myös lohkoketjun ensimmäiset käyttötarkoitukset liittyivät taloudellisiin palveluihin. Taloudellinen palvelu on perinteisimmillään arvon lähettämistä toimijalta toiselle, johon esimerkiksi myös virtuaalivaluutat perustuvat. On kuitenkin edelleen korostettava, että virtuaalivaluutat eivät ole ainoa luonteva käyttökohde lohkoketjulle. Nykyään lohkoketju koskettaa lähes kaikkia liiketoiminnan osa-alueita, ja uusia käyttötarkoituksia syntyy koko ajan lisää. Rahoituspalveluita tarjoavat instituutiot ovat tällä hetkellä pisimmällä lohkoketjun omaksumisessa osaksi liiketoimintaa (Iansiti & Lakhani, 2017), joten aikaisempia käyttötapauksia löytyy jonkin verran.

Ennen kuin lohkoketjuteknologian käyttötarkoituksiin rahoituspalveluissa voidaan paneutua, tulee itse rahoituspalvelut määritellä käsitteenä. Tässä tutkielmassa rahoituspalvelut rajataan kattamaan pankkien ja muiden rahalaitosten välittämän rahoituksen sekä sitä palvelevan toiminnan, lukuun ottamatta vakuutus- ja eläkepalveluita. Rahoituspalveluita voivat näin ollen olla esimerkiksi maksuliikenne, arvopaperipörssit, eri sijoitusmuodot ja myös edellisiä tukevat toiminnot. Erilaisia tähän määritelmään sopivia käyttökohteita on lukuisia, joten tässä tutkielmassa on syytä tarkastella lähinnä muutamaa merkittävintä ja lohkoketjun kannalta realistisinta käyttökohdetta.

5.1 Rahaliikenne

5.1.1 Virtuaalivaluutat

Kenties tunnetuin ja helpoin esimerkki lohkoketjuteknologian hyödyntämisestä rahaliikenteessä on virtuaalivaluutat. Maailmanlaajuinen talousjärjestelmä on teknologisen kehityksen mukana siirtynyt vähitellen kohti digitaalisempaa toimintaympäristöä, ja sen seurauksena on myös syntynyt erilaisia digitaalisen vaihdannan yksikköjä eli virtuaalivaluuttoja. Ilman virtuaalivaluuttojakin suurin osa

maailman niin kutsutusta fiat-rahasta[14] on keskuspankkien ja muiden instituutioiden tilikirjoissa keskitetyissä tietokannoissa, eli rahajärjestelmä on ainakin osittain digitalisoitunut. Talousjärjestelmä on kuitenkin rakentunut vuosikymmeniä kypsyneiden teknologioiden päälle, joten täysin uudenlaiset rahajärjestelmät ja vaihdantayksiköt tarvitsevat paljon aikaa ennen kuin ne voisivat vakiintua vanhojen tilalle.

Periaatteessa ensimmäinen virtuaalivaluutta oli DigiCash, jonka synty ajoittuu vuodelle 1989 (Johansson ym., 2019, s. 80), kauan ennen ensimmäistä lohkoketjua hyödyntävää virtuaalivaluuttaa bitcoinia. Suurin osa varhaisista virtuaalivaluutoista osoittautui kuitenkin epäonnistumisiksi ennen bitcoinia. Ensimmäinen toimiva pohja virtuaalivaluutalle oli lohkoketju, ja bitcoin on vielä tänäkin päivänä tunnetuin sekä käytetyin virtuaalivaluutta. Merkittävin muutos, jonka lohkoketjuteknologia toi mukanaan oli digitaalisen rahan kaksinkertaisen käytön ongelman ratkaiseminen. Digitaalisessa rahassa oli pitkään se ongelma, että yksittäistä rahayksikköä pystyi käyttämään useammin kuin kerran saman käyttäjän toimesta. Rahayksiköt muodostuvat vain digitaalisesta datasta, joten epärehellinen henkilö voi joissakin tilanteissa muokata sitä. Kuten fiat-rahan väärentäminen, virtuaalivaluutan kaksinkertainen käyttö johtaa rahan inflaatioon ja luottamuksen romahtamiseen valuuttaa kohtaan. Ennen lohkoketjua eri virtuaalivaluuttoja oli käytännössä rajaton kopioitavissa oleva määrä, mikä on vastoin toimivan valuutan periaatteita. Transaktioita varten tarvittiin luotettu kolmas osapuoli, joka hallinnoi transaktioiden oikeellisuutta ja sitä, ettei samaa rahayksikköä käytetty uudestaan. Lohkoketjuteknologia ratkaisi tämän ongelman yhdistämällä hajautetun tietoverkon periaatteen PKI:n avulla tehtävään transaktioiden aikaleimaamiseen. Näin transaktioilla on todisteet kronologisesta järjestyksestään ja tiivistefunktioiden avulla transaktiot voidaan myös tunnistaa ja varmentaa.

Virtuaalivaluutat ovat matalimman kynnyksen soveltamiskohde lohkoketjuteknologialle, ja niiden avulla on jo voitu mahdollistaa välittömiä kansainvälisiä transaktioita ilman välikäsiä tai keskusviranomaisia. Lohkoketjun

[14] Fiat-raha on rahaksi vakiintunut vaihdannan väline eli valuutta, jolla usein ei ole itseisarvoa ja joka on valtion tai hallinnon sääntelemä.

hyödyntäminen maksuliikenteessä yleisesti onkin helpoin tapa esimerkiksi pankeille ja rahalaitoksille omaksua se. Lohkoketjun käyttökohteena virtuaalivaluutoilla on kuitenkin rajallinen potentiaali, sillä kyseessä on vain tietty yksittäinen käyttökohde, jota on vaikea itsessään kehittää pidemmälle. Tämä vaatisi kokonaan uudenlaisen rahajärjestelmän vakiintumisen nykyisen tilalle.

5.1.2 Maksujärjestelmät

Uusia lohkoketjulla toimivia digitaalisia maksujärjestelmiä julkaistaan jatkuvasti ennen kaikkea vähentämään käteisen tarvetta sekä tarjoamaan turvallinen tapa hallita asiakkaiden transaktioita (de Reuver, Verschuur, Nikayin, Cerpa & Bouwman, 2015). Lohkoketjuteknologiaa voidaan hyödyntää varsinkin pankkien välisissä transaktioissa, jotka tällä hetkellä nojaavat vahvasti pankkien välisiin sovitteluihin, erilliseen kirjanpitoon ja maksujen alullepanoon. Nykyiset järjestelmät ovat hyvin monimutkaisia, niihin uppoutuu paljon kustannuksia ja kansainvälisissä maksuosoituksissa voi mennä useampikin päivä saapua perille. Lohkoketjuteknologia voi tarjota tähän kustannustehokkaan ja nopean ratkaisun vertaisverkon avulla. (Ali, Ally, Clutterbuck & Dwivedi, 2020.) Seuraava todennäköinen ja looginen käyttökohde lohkoketjuteknologialle on pankkien ja rahalaitosten paikalliset ja yksityiset lohkoketjujärjestelmät, jotka korvaisivat nykyiset tilikirjat.

Aivan kuten TCP/IP:n tapauksessa, lohkoketjuteknologian kehitys voi edetä askel kerrallaan hallitummin suljetussa ympäristössä, kuin täysin avoimessa vertaisverkossa. Useat organisaatiot voisivat osallistua samaan lohkoketjujärjestelmään, joka käsittää sisällään esimerkiksi tilikirjat, kirjanpidon, maksujärjestelmät ja erilaiset digitaaliset sopimukset. Pörssiyhtiö Nasdaq on tehnyt yhteistyötä Chain.comin kanssa vuodesta 2015 asti, kun Nasdaq Linq -lohkoketju suoritti onnistuneen osaketransaktion ensimmäiselle asiakkaalleen Chain.comille. Nasdaq ja Citi ilmoittivat toukokuussa 2017 kehittäneensä Chain.comin lohkoketjun pohjalta integroidun maksujärjestelmän, joka tallentaa maksuohjeita hajautettuun tilikirjaan. (Iansiti & Lakhani, 2017; Johansson ym., 2019, s. 150.) Tällä hetkellä vastaavia maksujärjestelmiä ei ole laajalti käytössä, mutta aivan kuten Nasdaq, monet eri organisaatiot ovat ryhtyneet kehittämään lohkoketjuteknologiaa kohtaamaan omia tulevaisuuden tarpeitaan.

Yritykset ovat myös alkaneet hyödyntämään lohkoketjuteknologiaa tarjoamissaan järjestelmissä. Vuonna 2012 perustettu venture capital -pääomarahoituksella rahoitettu yritys Ripple rakensi alun perin toimintansa lohkoketjuteknologian päälle, mutta muutti myöhemmin arkkitehtuuriaan. Ripple tarjosi rahoitusinstituutiolle tuotteena maksujärjestelmää, joka tehostaisi pankkien välisiä maksuja ja helpottaisi älykkäiden sopimusten tekemistä. Esimerkiksi virtuaalivaluuttapörssi Kraken on tarjonnut säänneltyjä rahoituspalveluita yhteistyössä pankkien kanssa (Swan, 2015, s.12) ja ohjelmistoyritys R3 on myynyt tuotteena hajautettua tilikirjajärjestelmä Cordaa yrityksille ja taloudellisille instituutioille (Johansson ym., 2019, s. 146–147).

5.2 Pääomamarkkinat

Rahoitusmarkkinat on ollut tapana jakaa kahteen osaan, rahamarkkinoihin sekä pääomamarkkinoihin, rahoitusinstrumenttien maturiteetin mukaan. Rahamarkkinoille kuuluvat alle vuoden pituiset rahoitusinstrumentit ja tätä pidemmät pääomamarkkinoille. Pääomamarkkinat voidaan jakaa vielä pitkän koron markkinoihin eli joukkovelkakirjamarkkinoihin sekä osakemarkkinoihin. Rahoitusmarkkinat voidaan myös jakaa ensi- sekä jälkimarkkinoihin. Ensi- tai ensisijaismarkkinoilla yritykset voivat hankkia uutta omaa pääomaa osakeanneilla tai vierasta pääomaa velkakirjojen myynnillä. Jälki- tai toissijaismarkkinoilla voidaan käydä kauppaa osakkeista tai velkakirjoista, ja osakekaupat tehdään yleensä arvopaperipörssissä. (Knüpfer & Puttonen, 2018, s. 54.) Tässä alaluvussa keskitytään lähinnä lohkoketjuteknologian hyödyntämiseen kaupankäynnissä pääomamarkkinoilla.

5.2.1 Arvopaperikauppa

Lohkoketjuteknologiaa ei ole otettu vielä virallisesti käyttöön arvopaperikaupoissa, mutta monet pörssit ympäri maailmaa ovat alkaneet suunnitella lohkoketjuteknologiaa maksujärjestelmiensä ja arvopaperikauppapaikkojensa pohjaksi, kuten aikaisemmin mainittu Nasdaq Linq -lohkoketju. Nasdaqin lisäksi muun muassa ASX, NYSE, Tokyo Stock Exchange, Deutsche Börse ja intialainen Securities Exchange Board ovat alkaneet jo kehittämään lohkoketjuteknologiasovelluksia transaktioitaan varten (Johansson ym., 2019, s. 149). Nykyään osakekaupat ovat jo valmiiksi algoritmien

avulla pitkälle automatisoituja sekä tehokkaita. Tästä huolimatta kaupan eri osapuolet, kuten ostaja, myyjä ja viranomaiset joutuvat käymään muutaman päivän tai jopa viikon kestävän prosessin. Prosessiin kuuluu maksujen siirtoja, prosessointia, arvopaperisäilytyksiä ja sopimuksia, mitkä kuluttavat aikaa ja resursseja. (Iansiti & Lakhani, 2017; Johansson ym., 2019, s. 150.) Lohkoketjuteknologian mahdollistamat älykkäät sopimukset voisivat tarjota ratkaisun osakekauppojen ja pörssien tehokkuuden kasvattamiseksi. Älykkäät sopimukset pienentävät keskusviranomaisten ja välikäsien tarvetta, joten osakekaupan automatisoitu prosessi olisi itse transaktiojärjestelmän sisällä. Lisäksi lohkoketjuteknologia voisi yhdistää osapuolten erilliset tilikirjat samaksi hajautetuksi tilikirjaksi, joka prosessoi transaktioita automaattisesti ja osapuolet toimisivat vain niiden takaajina.

5.2.2 Digitaaliset poletit

Poletiksi eli rahakkeeksi kutsutaan kaikkia sellaisia esineitä, joilla on tiettynä hetkenä jotain rahallista arvoa. Fyysisiä poletteja voivat olla esimerkiksi rahapelien poletit, ruokapoletit, puhelinpoletit ja oikeastaan mikä muu vastaava, joilla saa vastineeksi jotain hyödykettä, oikeuksia tai etuuksia. Digitaaliset poletit toimivat täysin samalla periaatteella, mutta digitaalisesti esimerkiksi lohkoketjussa. Varallisuuden siirtämistä lohkoketjulle voidaan hyödyntää digitaalisten polettien avulla: tietty määrä sidotaan tiettyyn omaisuuserän arvoon. Digitaalisten polettien avulla voidaan siirtää oikeastaan mitä tahansa fyysisen tai digitaalisen maailman omaisuus- ja varallisuuseriä vertailtavaan muotoon lohkoketjussa. Tämän avulla periaatteessa lähes kaikkea fyysistä omaisuutta voidaan tavanomaisten arvopaperien ohella käyttää sijoitus- ja kauppakohteena. Esimerkiksi fyysinen kultaharkko voidaan jakaa digitaalisten polettien avulla digitaalisiin omistuseriin, jolloin sijoittaja voi todennettavasti omistaa ja sijoittaa palaan kultaharkosta ilman, että fyysisesti omistaa sitä. Saman esimerkin voi laajentaa myös osakkeisiin, kiinteistöihin, bonuspisteisiin tai vaikka postimerkkeihin. Digitaaliset poletit helpottavat myös suurten fyysisten omaisuuserien kaupoissa ja siirroissa. Esimerkiksi suurta määrää öljyä ei tarvitse liikuttaa pitkin jakelukanavaa, sillä omistusoikeus öljystä on jo siirtynyt digitaalisten polettien avulla. Fyysisen omaisuuden muuttamiseen digitaaliseksi liittyy kuitenkin haaste: digitaalisten polettien ajantasaista yhteyttä fyysiseen varallisuuserään on hyvin vaikea

ylläpitää, sillä fyysisen maailman muutokset eivät voi näkyä heti digitaalisessa maailmassa.

Ajatus digitaalisista poleteista on laajentunut myös käsitteeseen vaihtokelvoton digitaalinen poletti eli NFT (non-fungible token). NFT on lohkoketjuun tallennettu datayksikkö tai tiedosto, joka voi käsittää mitä tahansa digitaalista tietoa, kuten kuvia, videoita, ääntä tai taidetta. NFT:n taustalla on idea tiedon muuttamattomuudesta ja yksilöllisyydestä, mitkä ovat keskeisiä lohkoketjuteknologian ominaisuuksia. Lohkoketjun datan yksilölliset tiivisteet erottavat sen kopioista, joten NFT:n omistajalla on tekijänoikeuksista erillinen todiste omistajuudesta. NFT:n avulla voidaan paremmin todistaa ja siirtää asiakkaiden yksilölliset varallisuuserät, vaikka poletit ovat samankaltaisia keskenään. Lisäksi NFT tarjoaa mahdollisuuden käydä kauppaa myös epätavallisilla varallisuuserillä, esimerkiksi elokuvilla, musiikilla ja taiteella.

Arvopaperipoletti (security token) on digitaalinen arvopaperi, joka toimii lohkoketjussa. Sitä voidaan pitää tietynlaisena arvopaperijohdannaisena, sillä arvopaperipoletin arvo on sidottu johonkin olemassa olevaan omaisuuserään, kuten arvopaperiin. Tämä voisi osakemarkkinoilla mahdollistaa sen, että osakkeet voidaan pilkkoa yksittäisiä kappaleita pienempiin eriin samalla tavalla kuin rahasto-osuudet ja virtuaalivaluutat. Toistaiseksi arvopaperipoletteja on käytetty vain listaamattomiin osakkeisiin, mutta tulevaisuudessa niiden käyttökohteita voitaisiin laajentaa. Syksystä 2018 lähtien Asiakastieto, Nordea, OP Ryhmä, Privanet ja Tieto ovat alkaneet kehittämään lohkoketjuteknologiapohjaista liiketoimintaverkkoa, jonka sisällä voi käydä kauppaa listaamattomilla osakkeilla arvopaperipolettien avulla ja hallita osakerekisteriä digitaalisesti. (Johansson ym., 2019, s. 119.) Tällainen kehitys voi tulevaisuudessa mahdollistaa laajemman digitaalisten polettien omaksumisen myös Suomessa ja arvopaperikauppaa voisi käydä entistä monipuolisemmin. Suomen Yleisradio esimerkiksi myi ensimmäisen NFT-uutisensa 1,3 Ether virtuaalivaluuttaa vastaan maaliskuun loppupuolella vuonna 2021 (Hallamaa, 2021).

5.3 Rahoitusmuodot

Eräs mielenkiintoinen mutta spekulatiivinen vaihtoehtoinen rahoitusmuoto on kolikkoanti eli ICO (Initial Coin Offering). Kolikkoanti on verrattavissa osakeantiin tai listautumisantiin, joissa yritys laittaa liikkeelle osakkeitaan kaupankäynnin kohteeksi. Osakeanti tai listautumisanti on tapa yritykselle kasvattaa omaa pääomaa ja tuottaa omistajilleen arvoa. Kolikkoannissa ostaja ei kuitenkaan hanki osakkeita, vaan yrityksen liikkeelle laskemaa omaa virtuaalivaluuttaa tai digitaalisia poletteja. Tämän vuoksi kolikkoanti on osakeanteja huomattavasti suoraviivaisempi prosessi. Se ei ole vielä kohdannut juurikaan sääntelyä, sillä kolikkoanteja ei toistaiseksi ole järjestetty Suomessa. Kolikkoantia voidaan pitää myös joukkorahoituksen muotona. Kolikkoanti on kuitenkin riskialtis sijoitus, sillä sitä hyödyntävät usein kasvuyritykset ja sijoitusmuoto itsessään on vakiintumaton. (Johansson ym., 2019, s. 114.) Matalan sääntelyn ja epävarmuuden vuoksi ICO:a voidaan käyttää myös huijausmuotona: SEC (2017) erityisesti varoittaa sen käytöstä pump and dump -sijoitushuijauksissa.

Lohkoketjuteknologia soveltuu läpinäkyvän ja hajautetun tietoverkkorakenteensa avulla erityisesti ulkomaankaupan rahoitukseen. Nykyisellään kansainväliset kauppatransaktiot ovat erityisen ongelmallisia pienille ja keskisuurille yrityksille, sillä usein tällaisilla yrityksillä ei ole resursseja kattamaan kaikkia kuluja ja riskejä, mitä vaihtoketjuun liittyy. Sen sijaan lohkoketjun avulla voitaisiin kehittää toiminta-alusta, jonka kautta kaikki kauppatransaktioon osallistuvat osapuolet voivat läpinäkyvästi hallinnoida, seurata ja maksaa transaktioita samassa järjestelmässä. Yhdeksän eurooppalaisen pankin (Rabobank, Deutsche Bank, HSBC, KBC, Natixis, Nordea, Santander, Societé Generale ja UniCredit) yhdessä kehittämä We.trade-konsortio perustuu juuri edellä mainitulle ajatukselle ja sen tavoitteena on yksinkertaistaa pk-yritysten rajat ylittävää vaihdantaa Euroopassa. We.trade tarjoaa yrityksille läpinäkyvyyttä kauppatransaktioissa ja helpomman pääsyn ulkomaankaupan rahoitukseen. Käytännössä alusta tekee transaktiot täysin automatisoidusti ja näyttää niiden tilat reaaliajassa jokaiselle verkon toimijalle, joka voi olla esimerkiksi ostaja, myyjä, pankki tai kuljetusyritys. (Johansson ym., 2019, s. 151–152.)

5.4 Muutosvoima

Koko rahoitusala itsessään on jo pitkään ollut digitaalisessa murroksessa. Perinteisesti pankit ja rahoituslaitokset ovat tarjonneet rahoituspalveluitaan fyysisinä, mutta nykyään lähes kaikki palvelut toteutuvat jo digitaalisesti. Lisäksi kehitys on mahdollistanut rahoituspalveluiden tarjonnan laajentumisen pankkien ja rahoituslaitosten ulkopuolelle (Gomber, Kauffman, Parker & Weber, 2018). Potentiaalinen kehitys ei kuitenkaan ole vielä saavuttanut lakipistettään. Monet asiantuntijat uskovat, että lohkoketjuteknologia voi parhaimmillaan tuoda perustavanlaatuisen muutoksen koko talous- ja rahajärjestelmään (Iansiti & Lakhani, 2017). Virtuaalisen valuutan, hajautetun maksujärjestelmän ja älykkäiden sopimusten avulla voisi olla mahdollista luoda tulevaisuudessa täysin automatisoitu, läpinäkyvä ja reaaliaikainen transaktio- ja omaisuusverkosto. Tähän verkostoon voisi kuulua kaikki sen toimijat aina rahoituslaitoksista henkilöasiakkaisiin. Reaaliaikaiset transaktiot ja sopimukset takaisivat esimerkiksi tiedon sekä omaisuuserien jatkuvan seuraamisen pitkin sen jakelukanavia, ja pankit voisivat samalla seurata epäluotettavia toimijoita ja huijauksia vertaisverkossa.

Lohkoketjuteknologian tulevaisuuden käyttökohteet ovat rajattomat, mutta edellä mainitut perustavanlaatuiset muutokset eivät ole vielä ajankohtaisia. Varsinkin täysin automatisoidut järjestelmät ja hallinnot tuhoaisivat välittömästi lukuisia työpaikkoja sekä elinkeinoja, joten on realistisempaa tarkastella muutosta hitaana ja asteittaisena kehityksenä. Älykkäiden sopimusten ja lohkoketjuteknologian omaksumisessa ja oppimisessa kuluu itsessään paljon aikaa. Niiden laaja-alainen käyttö vaatii myös suuria hankintoja ja todella laajaa infrastruktuurimuutosta. Teknologian uutuus aiheuttaa myös siihen liittyviä teknisiä ongelmia, joita ei vielä ole edes tunnistettu. Sen sijaan muut neljännen teollisen vallankumouksen merkittävät teknologiat, kuten IoT ja pilvipalvelut, ovat helpottaneet hajautetun lohkoketjuteknologian kokeiluissa merkittävästi (Iansiti & Lakhani, 2017). Yhdistämällä nämä eri teknologiat keskenään voi mahdollisesti olla edellytys myös tuleville teknologisille murroksille.

6 YHTEENVETO

Tässä tutkielmassa tavoitteena on esitellä lohkoketjuteknologian laajoja käyttömahdollisuuksia rahoituspalveluissa sekä selvittää, miten sen eri ominaisuuksia voidaan hyödyntää rahoituspalveluiden toteuttamisessa tulevaisuudessa. Alustavat tutkimuskysymykset olivat:

1) Mitä lohkoketjuteknologia on?
2) Mitä eri ominaisuuksia lohkoketjuteknologialla on, eli mitä vahvuuksia ja haasteita lohkoketjuteknologia kohtaa?
3) Miten lohkoketjuteknologiaa on jo hyödynnetty rahoituspalveluissa, ja miten sitä voidaan tulevaisuudessa hyödyntää enemmän?

Lohkoketjua voidaan kuvailla hajautetuksi tilikirjaksi, joka toimii vertaisverkossa. Sen toimivuus perustuu konsensusprotokollaa ylläpitävien solmujen yhdessä jakamaan kopioon lohkoketjun datasta, jota ei voida kryptografisen varmennuksen jälkeen enää muuttaa tai poistaa. Lohkoketju koostuu dataa sisältävistä lohkoista, jotka on ketjutettu toisiinsa kryptografisten tiivisteiden avulla. Lohkon sisäiset tiedot ovat salattu digitaalisilla allekirjoituksilla julkisen avaimen salausta eli PKI:tä hyödyntäen. Lisäksi lohkon tiedot on kronologisesti varmennettu tiivisteiden avulla, jotta verkon käyttäjät voivat olla varmoja tietojen oikeellisuudesta. Hajautetulle vertaisverkolle ominaisesti lohkoketjussa ei ole yhtä yksittäistä keskusviranomaista tai keskuspalvelinta, joten tieto siirtyy verkossa suoraan vertaisilta vertaisille. On olemassa sekä julkisia että yksityisiä lohkoketjuja, joiden suurin ero koskee avoimuutta liittyä verkkoon. Yksityiset lohkoketjut soveltuvat paremmin esimerkiksi pankkien ja rahoituslaitosten käyttöön, ja niiden konsensuksen ylläpitäminen keskitetysti on huomattavasti julkisia lohkoketjuja helpompaa. Julkisissa lohkoketjuissa konsensusalgoritmia toteuttaville solmuille on olemassa erilaisia kannustimia, kuten louhimispalkkioita, jotka voivat olla lohkoketjun ylläpitämää omaa virtuaalivaluuttaa.

Lohkoketjuteknologiassa yhdistyvät erityisesti avoimuus, luottamus, turvallisuus ja eheys. Hajautettu toimintaympäristö takaa käyttäjien välisen kryptografisen luottamuksen ilman välikäsiä, ja verkon toiminta voi parhaimmillaan olla avointa ja läpinäkyvää kaikille. Ilman keskitettyä palvelinta tai tietokantaa verkon osallistujien

tiedot ovat paremmin turvassa tuhoutumiselta tai pahantahtoisilta toimijoilta. Vaikka tieto on jaettu lohkoketjussa läpinäkyvästi ja hajautetusti, on se silti konsensusprotokollan avulla turvassa tarkoituksellisilta väärennöksiltä ja epävarmuudelta. Lohkoketjun tieto on näin ollen eheää. Uutena teknologiana lohkoketju kuitenkin kohtaa epävarmuuteen liittyviä pelkoja eri teknisistä ongelmista, hitaasta omaksumista ja mahdollisesta sääntelystä johtuen. Lohkoketjuun liittyvät vahvuudet ja haasteet määrittelevät pitkälti sen, mihin käyttökohteisiin se parhaiten rahoituspalveluissa soveltuu.

Lohkoketjuteknologian hajautettu tietoverkkorakenne on jo erityisesti mahdollistanut nopeita ja läpinäkyviä virtuaalivaluuttatransaktiota. Tämä käyttökohde voi tulevaisuudessa laajentua myös kattamaan erilaisia maksujärjestelmiä, kuten pankkien omia tilikirjakonsortioita. Älykkäiden sopimusten avulla voitaisiin rakentaa täysin automatisoituja lohkoketjuarvopaperikauppoja, joissa koko osaketransaktioprosessi muuttuu nykyistä tehokkaammaksi. Lisäksi digitaaliset poletit voivat mahdollistaa nykyistä monipuolisemman skaalan erilaisia kaupankäyntikohteita. Lohkoketjuteknologia on myös mahdollistanut digitaalisten polettien avulla entistä monipuolisemmat sijoitus- ja rahoituskohteet. ICO:n avulla on voitu muuttaa käsitystä yritysten listautumisanneista ja esimerkiksi ulkomaankaupan rahoitusta on jo helpotettu lohkoketjujärjestelmän avulla. Kaiken kaikkiaan lohkoketjulla on potentiaalia muuttaa kokonaisia hallinto- ja rahajärjestelmärakenteita, mutta se vaatisi todella pitkäaikaisen omaksumisen. Lisäksi lohkoketjuteknologia kohtaa erityisesti fyysisen ja digitaalisen omaisuuden perustavanlaatuiseen eroon liittyviä ongelmia, etenkin fyysisessä maailmassa tapahtuvien muutosten takia.

Edellä esiteltyjen tutkimuskysymysten päätulosten kautta voidaan vahvistaa yleinen käsitys siitä, että lohkoketjuteknologialle löytyy laajasti erilaisia käyttömahdollisuuksia rahoituspalveluista sekä suuri todennäköisyys tulla laajemmin omaksutuksi sen vahvuuksien vuoksi. Modernissa markkinataloudessa erilaiset tilikirjat ja rekisterit ovat keskeisessä asemassa, joten niiden muuttaminen lohkoketjupohjaiseksi voidaan nähdä jokseenkin luontaisena siirtymänä. Tutkielmassa esitetyt nykyiset käyttökohteet on todettu jo toimiviksi ratkaisuiksi, ja potentiaalisten käyttökohteiden mahdollisuudet tukevat aikaisempaa tutkimusta sekä trendejä teknologian vaiheittaisesta omaksumisesta. Lohkoketjua voidaan pitää monella tapaa

perustavanlaatuisena teknologiana, ja aiheeseen liittyvän kirjallisuuden tutkimuksesta huomataan selkeästi koko ajan laajentuvat käyttökohteet ja suurta potentiaalia odottavat asenteet. Vain muutamia vuosia vanhassa kirjallisuudessa esiintyviin teknisiin ongelmiin on jo tämän tutkielman tekohetkeen mennessä löytynyt ratkaisuja esimerkiksi uusien konsensusalgoritmien kautta. Mikäli lohkoketjun näkee perustavanlaatuisena teknologiana, kuten internetin, on sitä tarpeellista myös peilata historiaan. Tämän vuoksi tässä tutkielmassa vertaillaan sekä nykyisiä, että myös tulevia lohkoketjun käyttökohteita rahoituspalveluissa.

Tämä tutkielma tarjoaa lukijalleen yksinkertaistetun, mutta kattavan kuvan lohkoketjuteknologiasta sekä sen ominaisuuksista paneutumatta kuitenkaan monimutkaiseen ohjelmointiin lohkoketjun takana. Aikaisempaa suomenkielistä tieteellistä kirjallisuutta on vain vähän, joten uusia käsityksiä ja erilaisia lähteitä yhdistämällä saadaan luotua ajankohtainen lisä osaksi suomenkielistä tutkimusta lohkoketjusta. Kirjallisuustutkimuksessa on tutkittu eri lähteet hyvin tarkkaan ja monipuolisesti, jotta vältyttäisiin esimerkiksi tiedon muuttumiselta käännettäessä tekstiä englannista suomen kielelle. Yksi tämän tutkielman rajoituksista onkin lohkoketjuun liittyvät vakiintumattomat termit, käsitteet ja teoria. Tutkielmassa esiintyviä tuloksia eli käyttökohteita voidaan hyödyntää suoraan rahoitusalalla tällä hetkellä tai tulevaisuudessa. Tämä tutkielma ei anna ohjausta rahoituspalveluiden toteutusta vastaavissa päätöksissä, mutta se antaa yleistetysti tietoa lohkoketjun eri ominaisuuksista sekä mahdollisuuksista.

Mahdollinen jatkotutkimusaihe voisi olla rahoituspalveluissa omaksuttujen lohkoketjujen vertailu aikaisemmin käytettyihin teknologioihin sekä järjestelmiin esimerkiksi historiallisen datan valossa. Lisäksi lohkoketjuteknologian sisäisen ohjelmoinnin tarkempi tarkastelu olisi mielenkiintoinen tutkimusaihe, tosin se kuuluu enemmän tietotekniikan ja tietojenkäsittelytieteiden piiriin. Rahoituksen tutkimuksessa ehkä kunnianhimoisin jatkotutkimusaihe olisi kokonaan lohkoketjuteknologialle sekä älykkäille sopimuksille perustuvan raha- ja talousjärjestelmän mahdollistavien tekijöiden laadullinen tutkimus.

LÄHTEET

Ali, O., Ally, M., Clutterbuck & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management*, *54*. doi:10.1016/j.ijinfomgt.2020.102199

Benzel, K., Graff, S. B., Rakic, Y. & Watts, E. (2010). *The art of the Ancient Near East: A resource for educators*. New York: The Metropolitan Museum of Art.

Bitcoin. (2021). *Frequently asked questions.* Haettu osoitteesta https://bitcoin.org/en/faq#general

Blockchain.com. (2021). *Average Transactions Per Block*. Haettu osoitteesta https://www.blockchain.com/charts/n-transactions-per-block

Bower, J. L. & Christensen, C. M. (1995). Disruptive technologies: Catching the wave. *Harvard Business Review*, *73*(1), 44–53. Haettu osoitteesta https://hbr.org/1995/01/disruptive-technologies-catching-the-wave

de Reuver, M., Verschuur, E., Nikayin, F., Cerpa, N. & Bouwman, H. (2015). Collective action for mobile payment platforms: A case study on collaboration issues between banks and telecom operators. *Electronic Commerce Research and Applications*, *14*(5), 331–344. doi:10.1016/j.elerap.2014.08.004

de Vries, A. (2021). *Bitcoin Energy Consumption Index*. Haettu osoitteesta https://digiconomist.net/bitcoin-energy-consumption

Deloitte Development LLC. (2020). *Deloitte's 2020 Global Blockchain Survey*. Haettu osoitteesta https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C. & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, *30*(7), 1366–1385. doi:10.1109/TKDE.2017.2781227

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.

Gomber, P., Kauffman, R. J., Parker, C. & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems, 35*(1), 220–265. doi:10.1080/07421222.2018.1440766

Hallamaa, T. (26.3.2021). Ylen ensimmäinen NFT myytiin 1,3 etherillä – Mitä opimme matkasta kryptotaiteen maailmaan? *YLE*. Haettu osoitteesta https://yle.fi/uutiset/3-11857336

Iansiti, M. & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118–127. Haettu osoitteesta https://hbr.org/2017/01/the-truth-about-blockchain

Jensen, M. C. (1993). The modern industrial revolution, exit, and the failure of internal control systems. *The Journal of Finance*, *48*(3), 831–880. doi:10.1111/j.1540-6261.1993.tb04022.x

Johansson, P. E., Eerola, M., Innanen, A. & Viitala, J. (2019). *Lohkoketju: tiekartta päättäjille*. Helsinki: Alma Talent Oy.

Korkeimman hallinto-oikeuden vuosikirjapäätös 2019:42.

Knüpfer, S. & Puttonen, V. (2018). *Moderni rahoitus.* (10. uud. painos). Helsinki: Alma Talent Oy.

Lauslahti, K., Mattila, J. & Seppälä, T. (2016). Smart contracts: How will blockchain technology affect contractual practices? *Etla Reports, 68*, 1–27. Haettu osoitteesta https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-68.pdf

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Haettu osoitteesta https://bitcoin.org/bitcoin.pdf

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T. & Dutkiewicz, E. (2019). Proof-of-Stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access*, *7*, 85727–85745. doi:10.1109/ACCESS.2019.2925010

Puthal, D. & Mohanty, S. P. (2019). Proof of Authentication: IoT-friendly blockchains. *IEEE Potentials*, *38*(1), 26–29. doi:10.1109/MPOT.2018.2850541

Rivest, R. L. (1990). Cryptography. Teoksessa J. van Leeuwen (toim.), *Handbook of theoretical computer science: Vol. A* (s. 717–755). Amsterdam: Elsevier. doi:10.1016/B978-0-444-88071-0.50018-7

Rooney, K. (6.6.2018). SEC chief says agency won't change securities laws to cater to cryptocurrencies. *CNBC*. Haettu osoitteesta https://www.cnbc.com/amp/2018/06/06/sec-chairman-clayton-says-agency-wont-change-definition-of-a-security.html

Roubini, N. & Byrne, P. (2018). The blockchain pipe dream. *Project Syndicate*.

Schwab, K. (2017). *The fourth industrial revolution*. Haettu osoitteesta https://books.google.fi/books?id=ST_FDAAAQBAJ&printsec=copyright&hl=fi&source=gbs_pub_info_r#v=onepage&q&f=false

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Sebastopol, CA: O'Reilly Media, Inc.

The SEC's Office of Investor Education and Advocacy. (2017). *Investor alert: Public companies making ICO-Related claims*. Haettu osoitteesta https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/investor-25

Tuloverolaki 30.12.1995/1535.

Visa Inc. (2021a). *Visa acceptance for retailers*. Haettu osoitteesta https://usa.visa.com/run-your-business/small-business-tools/retail.html

Visa Inc. (2021b). *Digital currency comes to Visa's settlement platform*. Haettu osoitteesta https://usa.visa.com/visa-everywhere/blog/bdp/2021/03/26/digital-currency-comes-1616782388876.html